

(12)特許協力条約に基づいて公開された国際出願

10/522176

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2004年2月5日 (05.02.2004)

PCT

(10) 国際公開番号
WO 2004/012085 A1

- (51) 国際特許分類: G06F 12/14,
G11B 20/10, G06F 3/06, H04N 5/91
- (21) 国際出願番号: PCT/JP2003/009414
- (22) 国際出願日: 2003年7月24日 (24.07.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2002-216750 2002年7月25日 (25.07.2002) JP
- (71) 出願人 (米国を除く全ての指定国について): 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP];

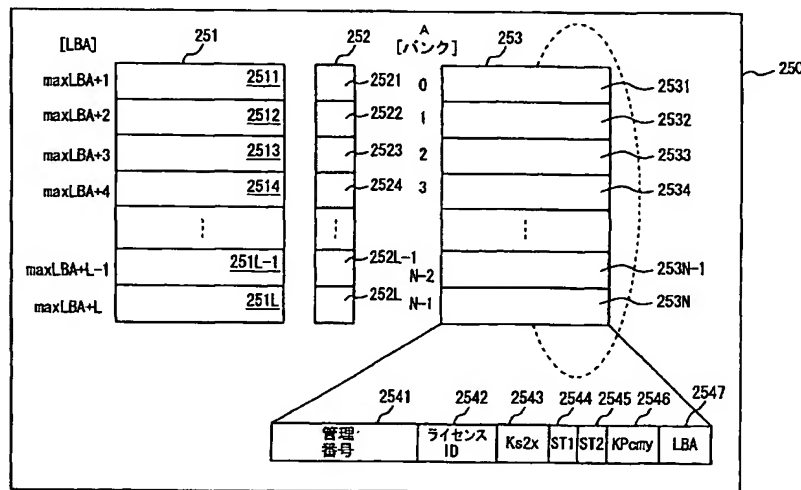
〒570-8677 大阪府 守口市 京阪本通2丁目5番5号 Os-
aka (JP). パイオニア株式会社 (PIONEER CORPORA-
TION) [JP/JP]; 〒153-8654 東京都 目黒区 目黒 1 丁目
4 番 1 号 Tokyo (JP). 株式会社日立製作所 (HITACHI,
LTD.) [JP/JP]; 〒101-8010 東京都 千代田区 神田駿河
台四丁目 6 番地 Tokyo (JP). フェニックステクノロ
ジーズ株式会社 (PHOENIX TECHNOLOGIES, K.K.)
[JP/JP]; 〒100-0005 東京都 千代田区 丸の内 1 丁目 3 番
地 1 東京銀行協会ビル 1 4 階 Tokyo (JP). 富士通株式
会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川
県 川崎市 中原区 上小田中 4 丁目 1 番 1 号 Kanagawa
(JP).

- (72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 堀 吉宏
(HORI, Yoshihiro) [JP/JP]; 〒570-8677 大阪府 守口
市 京阪本通2丁目5番5号 三洋電機株式会社内

[続葉有]

(54) Title: Data storage device capable of storing multiple SETS of history information on input/output processing of security data without duplication

(54) 発明の名称: 機密データの入出力処理に関する履歴情報を重複することなく複数格納できるデータ記憶装置



A...BANK
2541...MANAGEMENT NUMBER
2542...LICENSE ID

(57) Abstract: A data storage device comprises a secure data storage unit (250) including a log memory (253). The log memory (253), composed of multiple banks (2531 to 253N), stores history information in the multiple banks (2531 to 253N) in a ring. Each of the multiple banks (2531 to 253N) is specified by an address (0 to N-1). The history information stored in each of the banks (2531 to 253N) comprises a management number area (2541), a license ID (LID) area (2542), a Ks2x area (2543), an ST1 area (2544), an ST2 area (2545), a KPcm area (2546), and an LBA area (2547).

(57) 要約: データ記憶装置は、ログメモリ (253) を含むセキュアデータ記憶部 (250) を備える。ログメモリ (253) は、複数のバンク (2531~253N) から成り、複数のバンク (2531~253N) にリング状に履歴情報を格納する。複数のバンク (2531~253N) の各々は、

[続葉有]

WO 2004/012085 A1



Osaka (JP). 多田 謙一郎 (TADA, Kenichiro) [JP/JP]; 〒359-8522 埼玉県 所沢市 花園 4 丁目 2 6 1 0 番地 パイオニア株式会社 所沢工場内 Saitama (JP). 平井 達哉 (HIRAI, Tatsuya) [JP/JP]; 〒215-0013 神奈川県 川崎市 麻生区 王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内 Kanagawa (JP). 津留 雅文 (TSURU, Masafumi) [JP/JP]; 〒100-0005 東京都 千代田区 丸の内 1 丁目 3 番地 1 東京銀行協会ビル14階 フェニックステクノロジー株式会社内 Tokyo (JP). 長谷部 高行 (HASEBE, Takayuki) [JP/JP]; 〒211-8588 神奈川県 川崎市 中原区 上小田中 4 丁目 1 番 1 号 富士通株式会社内 Kanagawa (JP).

(74) 代理人: 深見 久郎, 外 (FUKAMI, Hisao et al.); 〒530-0054 大阪府 大阪市 北区 南森町 2 丁目 1 番 2 9 号 三井住友銀行南森町ビル 深見特許事務所 Osaka (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU,

ID, IL, IN, IS, KE, KG, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

2 文字コード及び他の略語については、定期発行される各 PCT ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明細書

機密データの入出力処理に関する履歴情報を
重複することなく複数格納できるデータ記憶装置

5

技術分野

この発明は、機密データの読出処理および書込処理を安全に提供するデータ記憶装置に関し、特に、著作権保護を可能とするデータ配信システムを用いて取得された暗号化データを復号および再生するためのライセンスを記憶し、マルチアクセスが可能なデータ記憶装置においてコピーされた情報に対する著作権保護を可能とするデータ記憶装置に関するものである。

10

背景技術

近年、インターネット等のデジタル情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

15

このようなデジタル情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

20

したがって、このようなデジタル情報通信網上において音楽データや画像データ等の著作権者の権利が存在するコンテンツが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

25

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

しかし、音楽データや画像データ等のコンテンツデータをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

この場合、デジタル情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンスを送信する。ライセンスは、暗号化コンテンツデータを復号するための復号鍵（「コンテンツ鍵」と言う。以下同じ。）、ライセンスを識別するためのライセンスID、およびライセンスの利用を制限するための制御情報等を含んでいる。配信サーバからメモリカードに対してライセンスを送信する際には、配信サーバおよびメモリカードは、それぞれがセッション鍵を生成し、配信サーバとメモリカードとの間で鍵の交換を行なうことによって、暗号通信路を構築し、配信サーバはメモリカードに対して構築した暗号通信路を介してライセンスを送信する。その際、メモリカードは、受信した暗号化コンテンツデータとライセンスとを内部のメモリに記憶する。

メモリカードに記憶した暗号化コンテンツデータを再生する場合は、メモリカードを携帯電話機に装着する。最終的に、携帯電話機は、通常の通話機能の他にメモリカードから暗号化コンテンツデータとコンテンツ鍵を読み出して暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。ライセンス鍵の読み出しに際しては、メモリカードと専用回路との間に暗号通信路を構築し、暗号通信路を介してメモリカードから専用回路に送信される。

また、メモリカードは、他のメモリカードとの間でライセンスの移動または複

製を行なう機能を備えている。この場合、配信サーバからライセンスの送信と同様に、送信元のメモリカードと送信先のメモリカードの双方の機能によって暗号通信路を構築した上で、ライセンスが送信元のメモリカードから送信先のメモリカードに対して送信される。ライセンスを移動するか複製するかは、ライセンス

5 に含まれる制御情報に従って決定される。

さらに、送受信中の不慮の中断によってライセンスが消失した場合に、その処理を再開でき、かつ、ライセンスの重複送信を防ぐためにライセンスの入出力に関する直近の履歴情報を記録し、必要に応じて出力する機能をメモリカードは備えている。送信元である配信サーバあるいはメモリカードは、送信先のメモリカードから履歴情報を取得して、この履歴情報に従ってライセンスの送受信の再開を判断する。履歴情報は、ライセンスIDと送受信を示すステータス情報を含ん

10 でいる。

このように、携帯電話機のユーザは、携帯電話網を用いて暗号化コンテンツデータとライセンスとを配信サーバから受信し、メモリカードに記憶したうえで、メモリカードに記憶された暗号化コンテンツデータを再生したり、他のメモリカードに移したりできる。また、著作権者の権利を保護することができる。

15

しかし、従来のメモリカードにおいては、直近の履歴情報を保持するのみで、中断後、他のライセンスに対する送受信を行った場合に先の中断に対する履歴情報が消えてしまう。このような場合、複数の履歴情報を格納することにより、ユーザの利便性を改善することが可能である。

20

また、記憶素子に対するアクセスの高速化や、記憶素子の大容量化に伴い、複数のライセンスの送受信を並行して行なう要求が発生することが、今後、予想される。その場合、少なくとも並行して行われる処理に関する履歴情報を格納できるようにする必要性が生ずる。

このように、複数の履歴情報を格納できるようにする場合に、ライセンスの受信後に、該ライセンスを他のメモリカードに対して移したとすると、同一のライセンスIDに対して異なったステータスを持つ履歴情報が格納されるという問題が生じる。

25

発明の開示

それゆえに、この発明の目的は、ライセンスに対して著作権を保護し、かつ、ライセンスの送受信を再開可能とするための履歴情報を重複することなく複数格納できるデータ記憶装置を提供することである。

5 なお、この発明は、コンテンツデータに対するライセンスに限られるものではなく、秘密にする必要がある機密データ一般に拡大され得る。

したがって、この発明によれば、データ記憶装置は、一定の手順に従って機密データの入出力を行ない、機密データを記憶し、かつ、一定の手順の進行に従って履歴情報を格納あるいは当該履歴情報を随時更新するデータ記憶装置であって、
10 外部とデータの入出力を行なうインターフェースと、複数の機密データを格納するデータ記憶部と、機密データの入出力に関する複数の履歴情報を格納するログ記憶部と、機密データの入出力を制御する制御部とを備え、ログ記憶部は、それぞれ1つの履歴情報を格納する2つ以上の領域を循環的に利用するリングバッファとして設けられており、ログ記憶部に記憶される複数の履歴情報の各々は、当該履歴情報を記憶した入出力対象の機密データを識別する識別情報を含み、制御部は、機密データの入出力の処理が開始されたことに伴い入出力の対象となった機密データを識別する識別情報をインターフェースを介して受取り、ログ記憶部の複数の領域を所定の順序で検索して、ログ記憶部に格納されている最も古い履歴情報を格納する領域を最古領域として特定し、その特定した最古領域に受取った識別情報を含む機密データの入出力処理に対する履歴情報を新たに格納する。
15 20

好ましくは、履歴情報の出力要求に対して履歴情報の一部または全てを出力する履歴情報の出力処理において、制御部は、入出力の対象となる機密データの識別情報をインタフェースを介して受取り、ログ記憶部の複数の領域を所定の順序で検索して、最古領域と、受取った識別情報を含む最も新しい履歴情報を格納する領域を最新領域として特定し、最新領域に格納されている履歴情報の一部または全てをインタフェースを介して出力する。
25

好ましくは、履歴情報の出力を伴う前記機密データの入力処理において、制御部は、入出力の対象となる機密データの識別情報をインタフェースを介して受取り、ログ記憶部の複数の領域を所定の順序で検索して、最古領域と、受取った識

別情報を含む最も新しい履歴情報を格納する最新領域とを特定し、その特定した最新領域に格納されている履歴情報の一部または全てを、特定した最古領域に複製することによって機密データの入力処理に対する新たな履歴情報として格納し、特定された最古領域に格納された履歴情報の一部または全てをインタフェースを介して出力する。

好ましくは、他の装置によって一定の手順の進行によって記録されたもう1つの履歴情報の入力を伴う機密データの再出力処理において、制御部は、入出力の対象となる機密データの識別情報およびもう1つの履歴情報とをインタフェースを介して受取り、最古領域および最新領域を特定し、その特定した最新領域に格納された履歴情報と、受取ったもう1つの履歴情報とに基づいて、機密データを出力するか否かを判定する。

好ましくは、他の装置によって一定の手順の進行に従って記録されたもう1つの履歴情報の入力を伴う機密データの出力処理において、制御部は、入出力の対象となる機密データの識別情報およびもう1つの履歴情報をインタフェースを介して受取り、最古領域および最新領域を特定し、その特定した最新領域に格納されている履歴情報の一部または全てを、特定した最古領域に複製することによって機密データの出力処理に対する新たな履歴情報として格納し、特定した最古領域に格納された履歴情報と、受取ったもう1つの履歴情報とに基づいて、機密データを出力するか否かを判定する。

好ましくは、最古領域を特定した後、制御部は、入出力処理における一定の手順が終了あるいは中止されるまでの間、特定された最古領域に格納された履歴情報を、当該手順の進行に従って随時更新する。

好ましくは、複数の履歴情報の各々は、ログ記憶部へ記憶された順序を識別するための管理番号をさらに含み、管理番号は、ログ記憶部に連続して配置された2つの領域に格納された2つの履歴情報に含まれる各々の管理番号に基づいて、古い履歴情報が格納される最古領域を検出する。

好ましくは、ログ記憶部は、 N (N は2以上の自然数) 個の領域を循環的に利用するリングバッファからなり、管理番号は、 M (M は、 $N < M$ を満たす自然数) の剰余系からなる。

好ましくは、制御部は、ログ記憶部に連続して配置された２つの領域に格納された２つの履歴情報に含まれる各々の管理番号を取得し、その取得した２つの管理番号の差に基づいて、２つの当該管理番号を含む２つの履歴情報が連続して格納されたか否かを判定し、２つの履歴情報が不連続に格納された履歴情報であるとき、連続する２つの領域のうち、後続領域を最古領域として検出する。

したがって、この発明によれば、機密データを保護し、かつ、機密データの入出力処理に関する複数の履歴情報を重複することなく格納し、出力あるいは参照できる。

10 図面の簡単な説明

図１は、データ配信システムを概念的に説明する概略図である。

図２は、図１に示すデータ配信システムにおいて送受信されるデータ、情報等の特性を示す図である。

図３は、図１に示すデータ配信システムにおいて使用される暗号通信に用いられる鍵、情報等の特性を示す図である。

図４は、図１に示すライセンス提供装置の構成を示す概略ブロック図である。

図５は、図１に示す端末装置の構成を示す概略ブロック図である。

図６は、図１に示す端末装置に装着されるハードディスクの構成を示す概略ブロック図である。

図７は、図６に示すハードディスクにおけるセキュアデータ記憶部の構成を示す図である。

図８は、図６に示すハードディスクにおけるノーマルデータ記憶部の構成を示す図である。

図９は、図１に示すデータ配信システムにおける配信処理を説明するための実施の形態１における第１のフローチャートである。

図１０は、図１に示すデータ配信システムにおける配信処理を説明するための実施の形態１における第２のフローチャートである。

図１１は、図９に示すステップＳ２０の詳細な動作を説明するためのフローチャートである。

図 1 2 は、図 1 1 に示すステップ S 2 0 a の詳細な動作を説明するためのフローチャートである。

図 1 3 は、図 1 に示すデータ配信システムにおける配信処理中の再書込処理を説明するための実施の形態 1 における第 1 のフローチャートである。

5 図 1 4 は、図 1 に示すデータ配信システムにおける配信処理中の再書込処理を説明するための実施の形態 1 における第 2 のフローチャートである。

図 1 5 は、図 1 に示すデータ配信システムにおける配信処理中の再書込処理を説明するための実施の形態 1 における第 3 のフローチャートである。

10 図 1 6 は、図 1 3 に示すステップ S 1 1 2 a の詳細な動作を説明するためのフローチャートである。

図 1 7 は、複製・移動処理が行なわれるシステム構成を概念的に説明する概略図である。

図 1 8 は、図 1 7 に示すシステムにおける複製または移動処理を説明するための実施の形態 1 における第 1 のフローチャートである。

15 図 1 9 は、図 1 7 に示すシステムにおける複製または移動処理を説明するための実施の形態 1 における第 2 のフローチャートである。

図 2 0 は、図 1 8 に示すステップ S 2 1 8 の詳細な動作を説明するためのフローチャートである。

20 図 2 1 は、図 1 7 に示すシステムにおける複製または移動処理中の再書込処理を説明するための実施の形態 1 における第 1 のフローチャートである。

図 2 2 は、図 1 7 に示すシステムにおける複製または移動処理中の再書込処理を説明するための実施の形態 1 における第 2 のフローチャートである。

図 2 3 は、図 1 7 に示すシステムにおける複製または移動処理中の再書込処理を説明するための実施の形態 1 における第 3 のフローチャートである。

25 図 2 4 は、図 5 に示す端末装置に対する再生許諾処理を説明するためのフローチャートである。

図 2 5 は、図 1 に示すデータ配信システムにおける配信処理を説明するための実施の形態 5 における第 1 のフローチャートである。

図 2 6 は、図 1 に示すデータ配信システムにおける配信処理を説明するための

実施の形態 5 における第 2 のフローチャートである。

図 27 は、図 25 に示すステップ S 16 a の詳細な動作を説明するためのフローチャートである。

5 図 28 は、図 17 に示すシステムにおける複製または移動処理を説明するための実施の形態 5 における第 1 のフローチャートである。

図 29 は、図 17 に示すシステムにおける複製または移動処理を説明するための実施の形態 5 における第 2 のフローチャートである。

図 30 は、図 28 に示すステップ S 208 の詳細な動作を説明するためのフローチャートである。

10

発明を実施するための最良の形態

本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

〔実施の形態 1〕

15 図 1 は、本発明によるデータ記憶装置が、暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのライセンスを取得するデータ配信システムの全体構成を概念的に説明するための概略図である。

20 なお、以下では、デジタル放送網により配信された映像データを端末装置 10 により受信して端末装置 10 に装着されたデータ記憶装置である HD（ハードディスクドライブ）20 に記憶し、また、暗号化された映像データを復号するためのライセンスを双方向のネットワーク 30 に端末装置 10 と接続されるライセンス提供装置 40 からネットワーク 30 を介してから受信して HD 20 に格納し、暗号化された映像データを端末装置 10 に内蔵された専用の再生回路（図示せず）にて再生するデータ配信システムの構成を例にとって説明する。一方、以下
25 の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、音楽データ、教材データ、朗読データ、書籍データ、ゲームなどのプログラムが扱われる場合においても適用することが可能なものである。また、データ記憶装置についても同様で、ハードディスクに限定されることなく、他のデータ記憶装置、たとえばメモ

リカードなどにおいても適用することが可能である。

図1を参照して、端末装置10は、デジタル放送網により配信される、暗号化された映像データ（以下、コンテンツデータとも呼ぶ）をアンテナ11を介して受信し、HD20に記憶する。暗号化されたコンテンツデータ（以下、暗号化コンテンツデータとも呼ぶ）を復号するためのコンテンツ鍵を含むライセンスを管理し、かつ、配信するライセンス提供装置40は、ライセンスの配信を求めてアクセスしてきた端末装置10に装着されたHD20が正当な認証データを持つか否か、すなわち、ライセンス管理機能を備えた正規のデータ記憶装置であるか否かの認証処理を行ない、HD20が正当なデータ記憶装置であった場合のみ、端末装置10に対してHD20においてのみ復号可能な所定の暗号方式によって暗号化したライセンスを送信する。そして、端末装置10は、ネットワーク30に接続されたモデムを介して暗号化されたライセンスを受信すると、その暗号化されたライセンスを装着されたHD20へ送信する。

図1においては、たとえば、HD20は、端末装置10に着脱可能な構成となっている。端末装置10に装着されたHD20は、端末装置10により受信された暗号化されたライセンスを受取り、著作権を保護するためにライセンス対してなされている暗号化を復号したうえでHD20内に記憶する。そして、ライセンスに対応した暗号化コンテンツデータを再生する場合、ライセンスに含まれるコンテンツ鍵と暗号化コンテンツデータとを端末装置10に与える。

そして、端末装置10のユーザは、端末装置10においてコンテンツ鍵を用いて復号されるコンテンツデータを再生することが可能となる。

このような構成とすることで、端末装置10のユーザは、ライセンス管理機能を備えた正規の認証データを有するHD20を利用しないと、暗号化されたコンテンツデータを受信して記憶したところでライセンスの提供を受けることができず、コンテンツデータを再生することができない。

なお、上述したデータ配信システムにおいては、暗号化コンテンツデータの提供元は、デジタル放送業者の放送サーバであるが、ライセンスを管理するライセンス提供装置40であってもよいし、インターネットなどの通信網を介して接続されるライセンス提供装置40とは別の配信サーバであってもよい。また、他の

ユーザからの複製であってもよい。すなわち、暗号化コンテンツデータ自体は、どこから発信されても、また、どこで受信されてもよく、要は暗号化コンテンツデータを復号可能なライセンスを厳重に管理しておきさえすれば、コンテンツデータの著作権を保護することができる。

- 5 したがって、本発明の実施の形態においては、HD 20、端末装置10およびライセンス提供装置40のそれぞれの間で行なわれるライセンスの送受信処理において、暗号化コンテンツデータを再生するために必要なライセンスの提供元が、提供先に対する認証およびチェック機能を行ない、非認証の装置に対するライセンスの出力を防止する。さらに、ライセンスの送受信処理中に異常が発生したとき、
- 10 ライセンスが重複して存在することがないように、再処理の必要なライセンスを特定することでコンテンツデータの著作権保護を実現しつつ、不慮の送受信処理の異常終了から回復可能なシステムの構成について説明する。

図2は、図1に示したデータ配信システムにおいて送受信されるデータ、情報等の特性を説明する図である。

- 15 データD_cは、コンテンツデータであって、ここでは映像データである。データD_cは、コンテンツ鍵K_cで復号可能な暗号化が施される。コンテンツ鍵K_cによって復号可能な暗号化が施された暗号化コンテンツデータE (K_c, D_c) が、この形式でデジタル放送網により端末装置10のユーザに配布される。

- なお、以下においては、E (X, Y) という表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。また、データD_cに付随して、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報D_iが配布される。
- 20

- また、ライセンスの配信を特定するとともに、各々のライセンスを特定する管理コードであるライセンスID (LID) が端末装置10を介してライセンス提供装置40とHD 20との間でやり取りされる。さらに、ライセンスとしては、データD_cおよびコンテンツ鍵K_cを識別するためのコードであるデータID (DID) や、利用者側からの指定によって決定されるライセンス数や機能限定など、データ記憶装置におけるライセンスや再生の取扱いに対する制限に関する制御情報ACが存在する。
- 25

コンテンツ鍵 K_c と、制御情報 AC と、 DID と、 LID とを併せて、以後、ライセンス LIC と総称することとする。 DID は、データ D_c とコンテンツ鍵 K_c との対に対して割り当てられた識別情報、すなわち、暗号化データ $E(K_c, D_c)$ を識別するための識別情報となる。 DID は、ライセンス LIC の他に、
5 暗号化データ $E(K_c, D_c)$ とともに常に扱われる付加情報 Di にも含まれ、参照できるようになっている。

図3は、図1に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

HD20などのデータ記憶装置および端末装置10などに備えられる再生回路
10 には、固有のクラス公開鍵 $KP_{cm y}$ および $KP_{cp y}$ がそれぞれ設けられ、クラス公開鍵 $KP_{cm y}$ および $KP_{cp y}$ は、データ記憶装置に固有のクラス秘密鍵 $K_{cm y}$ および再生回路に固有のクラス秘密鍵 $K_{cp y}$ によってそれぞれ復号可能である。これらクラス公開鍵およびクラス秘密鍵は、再生回路あるいはデータ記憶装置の種類ごとに異なる値を持ち、これらクラス公開鍵およびクラス秘密
15 鍵を共有する単位をクラスと称する。記号「 y 」は、そのクラスを識別するための識別子を表わす。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

また、データ記憶装置のクラス証明書として $C_{m y}$ が設けられ、再生回路のクラス証明書として $C_{p y}$ が設けられる。これらのクラス証明書は、データ記憶装置および再生回路のクラスごとに異なる情報を有する。
20

データ記憶装置のクラス証明書 $C_{m y}$ は、 $KP_{cm y} // I_{cm y} // E(K_a, H(KP_{cm y} // I_{cm y}))$ の形式で出荷時にデータ記憶装置に記憶され、再生回路のクラス証明書 $C_{p y}$ は、 $KP_{cp y} // I_{cp y} // E(K_a, H(KP_{cp y} // I_{cp y}))$ の形式で出荷時に再生回路に記憶される。ここで、 $X // Y$ は、 X と Y との連結を表わし、 $H(X)$ は、ハッシュ関数により演算されたデータ X のハッシュ値を表わす。マスタ鍵 K_a は、これらのクラス証明書を作成するために使用される秘密暗号鍵であり、このデータ配信システム全体で共通の秘密暗号鍵であって、認証局によって安全に管理運用される。また、クラス情報 $I_{cm y}$ 、 $I_{cp y}$ は、クラスごとの機器に関する情報およびクラス公
25

開鍵を含む情報データである。

また、 $E(K_a, H(KP_{cm_y} // I_{cm_y}))$ および $E(K_a, H(KP_{cp_y} // I_{cp_y}))$ は、それぞれ $KP_{cm_y} // I_{cm_y}$ および $KP_{cp_y} // I_{cp_y}$ に対する電子署名を行なった署名データである。

- 5 なお、認証局は、署名データを作成する公的な第三者機関であり、署名データ $E(K_a, H(KP_{cm_y} // I_{cm_y}))$ および $E(K_a, H(KP_{cp_y} // I_{cp_y}))$ は、認証局によって生成される。

さらに、データ記憶装置に対して安全かつ確実にライセンスLICを送信するための鍵として、データ記憶装置という媒体ごとに設定される個別公開鍵 KP_{om_z} と、個別公開鍵 KP_{om_z} で暗号化されたデータを復号することが可能な個別秘密鍵 K_{om_z} とが存在する。ここで、記号「z」は、データ記憶装置を個別に識別するための識別子である。

データ配信システムにおいてデータの送受信が行なわれるごとに、ライセンス提供装置40、データ記憶装置(HD20)、および端末装置10の再生回路において生成されるセッション鍵 K_{s1_x} 、 K_{s2_x} が用いられる。

ここで、セッション鍵 K_{s1_x} 、 K_{s2_x} は、ライセンス提供装置40、データ記憶装置(HD20)、もしくは端末装置10の再生回路間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵である。

「セッション」には、ライセンス提供装置40からデータ記憶装置(HD20)へライセンスを配信する「配信セッション」、データ記憶装置間でのライセンスの複製や移動を行なう「複製・移動セッション」、およびデータ記憶装置(HD20)から端末装置10の再生回路へライセンスを出力する「再生許諾セッション」がある。

これらのセッション鍵 K_{s1_x} 、 K_{s2_x} は、各セッションごとに固有の値を有することにより、ライセンス提供装置40、データ記憶装置(HD20)、および端末装置10の再生回路によって管理される。具体的には、セッション鍵 K_{s1_x} は、ライセンスを送受信する際に、ライセンスの送信側によってセッションごとに発生され、セッション鍵 K_{s2_x} は、ライセンスの受信側によってセッションごとに発生される。なお、記号「x」は、セッションにおける一連の処理

を識別するための識別子である。そして、各セッションにおいてこれらのセッション鍵を各機器間で相互に授受し、他の機器で生成されたセッション鍵を受けて、そのセッション鍵による暗号化を実行したうえで、ライセンスLIC、またはコンテンツ鍵を含むライセンスLICの一部の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

図4は、図1に示したライセンス提供装置40の構成を示す概略ブロック図である。

ライセンス提供装置40は、管理対象のライセンスを保持するデータベースであるコンテンツDB402と、ライセンスを配信する配信セッションにおける全ての通信記録を随時記憶し、保持するデータベースであるログDB404と、コンテンツDB402およびログDB404とバスBS1を介してデータをやり取りし、所定の処理を行なうためのデータ処理部410と、ネットワーク30を介して端末装置10とデータ処理部410との間でデータ授受を行なうための通信装置450とを備える。

データ処理部410は、バスBS1上のデータに応じて、データ処理部410の動作を制御するための配信制御部412と、配信制御部412により制御されて、配信セッション時にセッション鍵 K_{s1x} を発生するためのセッション鍵発生部414と、端末装置10から送られてくるHD20のクラス証明書 C_{my} に含まれる署名データ $E(K_a, H(KP_{cmy} // I_{cmy}))$ を復号するためのHD20の認証鍵 KPa を保持する KPa 保持部416と、HD20から送られてきたクラス証明書 C_{my} を通信装置450およびバスBS1を介して受け、 KPa 保持部416から受ける認証鍵 KPa によって復号処理を行ない、クラス証明書 C_{my} に含まれる署名データ $E(K_a, H(KP_{cmy} // I_{cmy}))$ の復号処理と、クラス証明書 C_{my} に含まれる $KP_{cmy} // I_{cmy}$ のハッシュ値の計算を行ない、両者の結果を比較チェックしてクラス証明書 C_{my} の検証を行なう認証部418と、配信セッションごとに、セッション鍵発生部414により生成されたセッション鍵 K_{s1x} を認証部418によってクラス証明書 C_{my} から抽出したクラス公開鍵 KP_{cmy} を用いて暗号化し、バスBS1に出力するための暗号処理部420と、セッション鍵 K_{s1x} によって暗号化された上で

送信されたデータをバスBS1より受け、復号処理を行なう復号処理部422とを含む。

データ処理部410は、さらに、配信制御部412から与えられるライセンスLICを、復号処理部422によって得られたデータ記憶装置ごとに固有な個別公開鍵K_{Pomz}によって暗号化するための暗号処理部424と、暗号処理部424の出力を、復号処理部422から与えられるセッション鍵K_{s2x}によってさらに暗号化してバスBS1に出力するための暗号処理部426とを含む。

なお、個別公開鍵K_{Pomz}およびセッション鍵K_{s2x}は、セッション鍵K_{s1x}によって暗号化されたうえで端末装置10から提供される。復号処理部422は、これを復号して個別公開鍵K_{Pomz}を得る。

ライセンス提供装置40の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

図5は、図1に示した端末装置10の構成を説明するための概略ブロック図である。

端末装置10は、デジタル放送網によって伝送される信号を受信するアンテナ102と、アンテナ102からの信号を復調してデータに変換、あるいはアンテナ102から送信するデータを変調してアンテナ102に与える受信部104と、端末装置10をネットワーク30に接続するモデム106と、端末装置10の各部のデータ授受を行なうバスBS2と、バスBS2を介して端末装置10の動作を制御するコントローラ108と、HD20とバスBS2との間のデータの授受を制御するHDインターフェース部110とを含む。

端末装置10は、さらに、上述したクラス証明書C_{py}を保持する認証データ保持部1502を含む。ここで、端末装置10のクラスを識別する識別子yは、y=3であるとする。

端末装置10は、さらに、クラス固有の復号鍵であるクラス秘密鍵K_{cp3}を保持するK_{cp}保持部1504と、バスBS2から受けたデータをクラス秘密鍵K_{cp3}によって復号し、HD20によって発生されたセッション鍵K_{s1x}を得る復号処理部1506とを含む。

端末装置10は、さらに、HD20に記憶されたコンテンツデータの再生を行

なう再生許諾セッションにおいて、HD 20との間でやり取りされるデータを暗号化するためのセッション鍵 K_{s2x} を乱数等により発生するセッション鍵発生部1508と、HD 20からコンテンツ鍵 K_c を受取る際に、セッション鍵発生部1508により発生されたセッション鍵 K_{s2x} を復号処理部1506によって得られたセッション鍵 K_{s1x} によって暗号化し、バスBS2に出力する暗号処理部1510と、バスBS2上のデータをセッション鍵 K_{s2x} によって復号して、コンテンツ鍵 K_c を出力する復号処理部1512と、バスBS2より暗号化コンテンツデータE(K_c , D_c)を受けて、復号処理部1512からのコンテンツ鍵 K_c によって暗号化コンテンツデータE(K_c , D_c)を復号してデータ D_c を再生部1516へ出力する復号処理部1514と、復号処理部1514からの出力を受けてコンテンツを再生するための再生部1516と、再生部1516の出力をデジタル信号からアナログ信号に変換するDA変換部1518と、DA変換部1518の出力をテレビモニターなどの外部出力装置(図示省略)へ出力するための端子1520とを含む。

なお、図5においては、点線で囲んだ領域は暗号化コンテンツデータを復号して映像データを再生する専用回路である再生回路150を構成する。再生回路150は、セキュリティを向上させるために1チップ構成の半導体デバイスであることが好ましい。さらには、再生回路150は、外部からの解析が困難な耐タンパモジュールとして構成されることが好ましい。

端末装置10の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

ここでは、端末装置10は、暗号化コンテンツデータを受信する機能、ライセンスの配信を受ける機能、再生許諾によって暗号化コンテンツデータを再生する機能を備えていたが、HD 20が端末装置10から脱着可能なデータ記憶装置であることから明らかなように、これらの機能を別々の装置によって実現してもよい。この場合、目的とする機能を実現する装置にHD 20を装着することで容易に実現できる。

図6は、図1に示すHD 20の構成を説明するための概略ブロック図である。

すでに説明したように、データ記憶装置であるHD 20には、クラス公開鍵 K

P c m y とクラス秘密鍵 K c m y のペア、および個別公開鍵 K P o m z と個別秘密鍵 K o m z のペアが設けられるが、HD 20 においては、これらを識別する識別子 $y = 1$ 、識別子 $z = 2$ で表されるものとする。

したがって、HD 20 は、クラス証明書 C m 1 として認証データ K P c m 1 /
5 / I c m 1 / / E (K a , H (K P c m 1 / / I c m 1)) を保持する認証データ保持部 202 と、クラス秘密鍵 K c m 1 を保持する K c m 保持部 204 と、個別秘密鍵 K o m 2 を保持する K o m 保持部 206 と、個別秘密鍵 K o m 2 によって復号可能な個別公開鍵 K P o m 2 を保持する K P o m 保持部 208 とを含む。

このように、データ記憶装置（ここでは HD 20）の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたコンテンツ鍵の管理をデータ記憶装置単位で実行することが可能になる。

HD 20 は、さらに、端末装置 10 の HD インターフェース部 110 と端子 210 を介して信号を授受する ATA (A T - A t t a c h m e n t) インターフェース部 212 と、HD 20 におけるデータ伝送路であるバス B S 3 と、ATA
15 インターフェース部 212 からコントローラ 214 を介してバス B S 3 に出力されたデータを、K o m 保持部 206 により与えられた個別秘密鍵 K o m 2 により復号し、ライセンス提供装置 40 から配信されたライセンス L I C をセキュアデータ記憶部 250 へ出力する復号処理部 216 と、K P a 保持部 218 から認証鍵 K P a を受け、バス B S 3 に出力されたデータの認証鍵 K P a による復号処理
20 を実行して復号結果をコントローラ 214 へ出力し、かつ、得られたクラス公開鍵 K P c m 1 を暗号処理部 222 へ出力する認証部 220 と、切換スイッチ 260 によって選択的に与えられるセッション鍵 K s 1 x または K s 2 x によって、切換スイッチ 262 によって選択的に与えられるデータを暗号化してバス B S 3 に出力する暗号処理部 224 とを含む。

25 HD 20 は、さらに、配信、複製・移動、および再生許諾の各セッションにおいて、セッション鍵 K s 1 x , K s 2 x を発生するセッション鍵発生部 226 と、セッション鍵発生部 226 の出力したセッション鍵 K s 1 x を認証部 220 によって得られる端末装置 10 の再生回路 150 のクラス公開鍵 K P c p y あるいは他のデータ記憶装置 (HD 21 とする) のクラス公開鍵 K P c m y によって暗号

化してバスBS3に送出する暗号処理部222と、バスBS3よりセッション鍵 $Ks2x$ によって暗号化されたデータを受けてセッション鍵発生部226より得たセッション鍵 $Ks1x$ または $Ks2x$ によって復号する復号処理部228とを含む。

5 HD20は、さらに、バスBS3上のデータをクラス公開鍵 $KPcm1$ と対をなすクラス秘密鍵 $Kcm1$ によって復号するための復号処理部230と、ライセンスLICをHD20からHD21へ移動または複製するために出力する際に、提供先のHD21から受信した個別公開鍵 $KPomz$ ($z \neq 2$) によりライセンスLICを暗号化する暗号処理部232とを含む。

10 HD20は、さらに、暗号化コンテンツデータE (Kc, Dc) を再生するためのライセンスLICと、HD20が処理しているセッションの処理記録であるログとをバスBS3より受けて記憶するセキュアデータ記憶部250を含む。そして、ライセンスLICは、セキュアデータ記憶部250内のライセンス領域に格納され、ログは、セキュアデータ記憶部250内のログメモリに格納される。

15 セキュアデータ記憶部250は、たとえば半導体メモリによって構成される。

図7は、セキュアデータ記憶部250におけるメモリ構成を示した図である。

図7を参照して、セキュアデータ記憶部250は、ライセンス領域251と、有効フラグ領域252と、ログメモリ253とを含む。

20 ライセンス領域251は、L個 (Lは自然数) の領域2511~251Lから成り、それぞれ1つのライセンス (コンテンツ鍵 Kc 、制御情報AC、ライセンスID (LID)、データID (DID)) を格納する。

25 領域2511~251Lに格納された複数のライセンスの各々は、アドレス (以下、 $LBA: Logical Block Address$ と称する。) によって管理される。そして、各セッションにおいて記憶あるいは読出されるライセンスLICは、全てLBAにより特定される。

領域2511~251Lに対応して $maxLBA+1 \sim maxLBA+L$ のLBAが付与されているものとする。たとえば、領域2513に格納されたライセンスLICは、 $LBA: maxLBA+3$ によって特定される。このとき、 $LBA: 0 \sim maxLBA$ は、ノーマルデータ記憶領域270に割当てられるものと

する。詳細は後述する。

なお、ライセンス領域 251 には、ノーマルデータ記憶領域 270 に割当てられた LBA (0 ~ max LBA) に続く値、すなわち、max LBA + 1 ~ max LBA + L が LBA として割当てられると説明したが、ライセンス領域 251 に割当てた L 個の LBA によって、それぞれが領域 2511 ~ 251L のいずれか 1 つを指定できる値であればいかなる値であってもよく、ノーマルデータ記憶領域 270 に割当てた LBA と重複する値、あるいは、独立した値を LBA として割当ててもよい。

また、有効フラグ領域 252 は、セキュアデータ記憶部 250 上の記憶位置を特定する LBA それぞれに対応して設けられ、対応する LBA によって特定される位置に記憶されるライセンスの有効性を示すフラグを記憶する。

有効フラグ領域 252 は、領域 2521 ~ 252L から成り、領域 2521 ~ 252L は、それぞれ、対応する領域 2511 ~ 251L に格納されたライセンス LIC の”有効”、または”無効”を格納する。

有効フラグ領域 252 のフラグが”有効”であるとき、フラグに対応する LBA によって特定されるセキュアデータ記憶部 250 上の記憶位置に記憶されているライセンス LIC は利用可能であり、ユーザはそのライセンス LIC 内のコンテンツ鍵 Kc を再生許諾によって読出して、対応する暗号化コンテンツデータを復号し、コンテンツデータを再生したり、そのライセンス LIC を他のデータ記憶装置に移動・複製することができる。

一方、有効フラグ領域 252 のフラグが”無効”であるとき、そのフラグに対応する LBA によって特定されるセキュアデータ記憶部 250 上の記憶位置に記憶されているライセンス LIC は利用不可であり、HD 20 のコントローラ 214 によって、その LBA からのライセンス LIC は拒否される。すなわち、消去されたのと同じ状態である。したがって、ユーザはそのライセンス LIC に対応したコンテンツデータを再生することはできない。この有効フラグ領域 252 のフラグは、ライセンスの新たな記憶によって”有効”とされ、ライセンスの移動によって”無効”とされる。

ログメモリ 2 5 3 は、ライセンスを HD 2 0 に入出力する場合の履歴情報（以下では「ログ」と呼ぶ。）を 1 つ格納する N (N は自然数) 個の領域 2 5 3 1 ~ 2 5 3 N からなるリングメモリである。領域 2 5 3 1 ~ 2 5 3 N は、それぞれ、バンク 0 ~ $N-1$ と称される領域を特定する名称が付与されている。したがって、

5 バンク n (n は N の剰余系) とは、ログメモリ上の領域 2 5 3 ($n-1$) を示す。

ログメモリ 2 5 3 は、複数のログをリング状に格納する。すなわち、ログメモリ 2 5 3 は、バンク 0 によって特定される領域 2 5 3 1 からログの格納を開始し、バンク $N-1$ によって特定される領域 2 5 3 N にログを格納すると、再びバンク 0 によって特定される領域 2 5 3 1 に戻り、ログを格納する。

10 バンク 0 ~ $N-1$ 、すなわち、ログメモリ 2 5 3 の領域 2 5 3 1 ~ 2 5 3 N の各々に格納されるログは、管理番号領域 2 5 4 1 と、ライセンス ID (L I D) 領域 2 5 4 2 と、 $K_s 2_x$ 領域 2 5 4 3 と、ST 1 領域 2 5 4 4 と、ST 2 領域 2 5 4 5 と、 $K P c m y$ 領域 2 5 4 6 と、L B A 領域 2 5 4 7 とを含む。

管理番号領域 2 5 4 1 は、ログをバンク 0 ~ $N-1$ の各々に格納する際に、ログの格納の順序を示す管理番号を格納する。そして、管理番号は、 M ($M > N$ 、 M は自然数) の剰余系をなして、昇順に付与される。この管理番号を格納することによって、最新のログを格納した、あるいは、最も古いログを格納したバンクを検索することができるようになる。すなわち、最初に管理番号 1 のログがバンク 0 に格納されるとすると、そのログの管理番号領域 2 5 4 1 は、管理番号”

20 1” を格納する。そして、ライセンスの入出力に伴い、新たなログを格納するとに、バンク 2 から順に使用し、そのログの管理番号領域 2 5 4 1 に、新たなログを格納するバンクの直前のバンクに格納される最新のログの管理番号領域 2 5 4 1 に格納される管理番号に 1 ずつ増加した管理番号を格納する。したがって、各バンク 0 ~ $N-1$ 、すなわち、領域 2 5 3 1 ~ 2 5 3 N に格納されたログの管理番号領域 2 5 4 1 から管理番号を読み出せば、管理番号に基づいてそのログが

25 新しいか古いかを判断できる。この判断は、次のようにして行なう。すなわち、連続する 2 つのバンク n 、 $n+1$ (n は N の剰余系) が保持する管理番号が不連続である場合、バンク n には最新のログが、バンク $n+1$ には最も古いログが保持されている。さらに、詳細な説明は、後述する。

以降では、特に断らない限り、管理番号に関する表記および演算は全てMの剰余系においてログメモリ253の領域2531~253Nを指定するバンクの番号に関する表記および演算は全てNの剰余系における表記および演算を示している。

5 ライセンスID領域2542は、セッションの対象となるライセンスLICを特定するライセンスID(LID)を格納する。Ks2x領域2543は、セッションにおいてライセンスLICの受信側のデータ記憶装置によって生成されたセッション鍵Ks2xを格納する。

10 ST1領域2544は、動作中のセッションにおける処理の状態を示すステータスST1を格納する。ST2領域2545は、ライセンスID領域2542に格納されるライセンスIDに対応したライセンスの記憶状態を示すステータスST2を格納する。

15 KPCmx領域2546は、ライセンスを移動・複製によって出力する場合、送信側のデータ記憶装置において受信側のデータ記憶装置のクラス公開鍵KPCmxを格納する。LBA領域2547は、各セッションにおいてライセンスLICを読み出あるいは記憶するために指示されたLBAを格納する。

20 一連のセッションの処理が進行するにつれて、上記各領域のデータが更新あるいは参照されていく。ステータスST1は、“受信待”、“受信済”、“送信待”および“送信済”の4状態のいずれかであり、ステータスST2は、“データ有”、“データ無”および“移動済”の3状態のいずれかである。

25 そして、セッション中に予期しない異常が発生し、セッションが中断した場合、そのセッションにおいて送受信されていたライセンスLICに対して、ログメモリ253内のライセンスID領域2541に格納されているライセンスIDと、LBA領域2547に格納されたLBAとによって当該ライセンスLICの記憶状態が確認され、その確認結果に応じてステータスST2が更新される。また、中断したセッションにおけるライセンスの送信側では、ライセンスの受信側のログメモリ253内に格納されているライセンスLIC、セッション鍵Ks2x、ステータスST1およびステータスST2を受取って、自身が記録するログの内容と受取ったライセンスLIC、セッション鍵Ks2x、ステータスST1およ

びステータス S T 2 とを確認することにより、再度のライセンスの送信を行なってもよいか否かの判断がされる。

5 なお、セッション鍵 K s 2 x は、各セッションを特定するために記憶され、セッション鍵 K s 2 x を共有していることは、ライセンスの送受信先およびその処理を共有していたことを示している。

 また、ステータス S T 2 には、出力ログが出力される際に、ログメモリ 2 5 3 に格納されているライセンス I D (L I D) と L B A とによってセキュアデータ記憶部 2 5 0 における対象のライセンスの記憶状態が格納され、これによって出力ログが成立する。

10 詳細については、後ほど各セッション毎のフローチャートを使用して説明する。

 再び図 6 を参照して、H D 2 0 のデータ記録部に関して説明する。H D 2 0 は、さらに、暗号化コンテンツデータを記憶するノーマルデータ記憶部 2 7 0 を含む。ノーマルデータ記憶部 2 7 0 は、データが記憶される円盤状の磁気記録媒体 2 7 0 1 と、磁気記録媒体 2 7 0 1 を回転させるモータ 2 7 0 2 と、モータ 2 7 0 2 を制御するサーボ制御部 2 7 0 3 と、磁気記録媒体 2 7 0 1 上における磁気ヘッドの位置を制御するシーク制御部 2 7 0 4 と、磁気ヘッドへデータの記録および再生を指示する記録再生処理部 2 7 0 5 とを含む。

 H D 2 0 は、さらに、A T A インターフェース部 2 1 2 を介して外部との間でデータ授受、制御情報 A C に基づくライセンスの出力に関する判断、およびセキュアデータ記憶部 2 5 0 の管理などの H D 2 0 内の動作を制御するためのコントローラ 2 1 4 を含む。

 なお、ノーマルデータ記憶部 2 7 0 、A T A インターフェース部 2 1 2 および端子 2 1 0 を除く他の構成は、耐タンパモジュール領域に構成される。

 図 8 を参照して、ノーマルデータ記憶部 2 7 0 の構成は、一般の公知のハードディスクの構成と変わるところはなく、データ記憶部 2 7 0 0 を含む。データ記憶部 2 7 0 0 は、領域 2 8 0 0 ~ 2 8 0 A (A = m a x L B A 、 m a x L B A は自然数) の各々は、暗号化コンテンツデータおよび暗号化コンテンツデータの付属データ、ライセンステーブル等を格納する。そして、領域 2 8 0 0 ~ 2 8 0 A に対応して L B A : 0 ~ m a x L B A が付与されており、各領域 2 8 0 0 ~ 2 8

0Aは、LBA：0～max LBAによって指定され、暗号化コンテンツデータ等のデータは、指定された各領域2800～280Aに入出力される。

5 なお、ライセンステーブルは、暗号化コンテンツデータとライセンスの関係を示す情報テーブルであり、ライセンステーブルを参照することで、暗号化コンテンツデータに対応するライセンスと、そのライセンスが記憶されているLBAを
10 特定することができる。したがって、ライセンステーブルは、暗号化コンテンツデータの記憶、削除時、あるいはライセンスの記憶、移動、削除時にその内容が変更される。

10 したがって、HD20は、LBA：0～max LBAによって指定できるノーマルデータ記憶部270と、それに続くLBA：max LBA+1～max LBA+Lによって指定できるセキュアデータ記憶部250、より具体的には、ライセンスメモリ251に対してデータあるいはライセンスの入出力が行なうことができる。

15 また、ノーマルデータ記憶領域270およびライセンス領域251に対するLBAの値については、本実施の形態に限るものではない。

20 なお、セキュアデータ記憶部250は、通常のアクセスコマンドではATAインタフェース部212を介して、直接、外部からアクセスできない等の手段を設けることで耐タンパ性を確保した、耐タンパ構造を備えている。

20 また、HD20のセキュアデータ記憶部250は、全て半導体メモリによって構成されるものとして説明したが、耐タンパ性を確保した上で、セキュアデータ記憶部250の一部あるいはその全てを、磁気記録媒体2701上に記憶する構成としてもよい。

25 以下、図1に示すデータ配信システムにおける各セッションの動作について説明する。

25 [配信]

25 まず、図1に示すデータ配信システムにおいて、ライセンス提供装置40から端末装置10に装着されたHD20へライセンスを配信する動作について説明する。

25 図9および図10は、図1に示すデータ配信システムにおいて、端末装置10

のユーザが端末装置 10 から暗号化コンテンツデータのライセンス配信のリクエストを行なうことにより、ライセンスがライセンス提供装置 40 から端末装置 10 に装着された HD 20 へ向けて送信され、HD 20 に記憶される際の処理（配信セッション）を説明するための第 1 および第 2 のフローチャートである。

5 図 9 における処理開始以前に、端末装置 10 のユーザは、端末装置 10 をモデム 106 によりネットワーク 30 に接続し、端末装置 10 をネットワーク 30 を介してライセンス提供装置 40 に接続していることを前提としている。

10 図 9 を参照して、端末装置 10 のユーザから所望のコンテンツデータのライセンスに対する配信リクエストがなされると、端末装置 10 のコントローラ 108 は、バス BS 2 および HD インターフェース部 110 を介して HD 20 へクラス証明書の出力要求を出力する（ステップ S 1）。HD 20 のコントローラ 214 は、端子 210 および ATA インターフェース部 212 を介してクラス証明書の出力要求を受理すると（ステップ S 2）、バス BS 3 を介して認証データ保持部 202 からクラス証明書 $Cm1 = KP_{cm1} // I_{cm1} // E(K_a, H(KP_{cm1} // I_{cm1}))$ を読み出し、クラス証明書 $Cm1$ を ATA インターフェース部 212 および端子 210 を介して端末装置 10 へ出力する（ステップ S 3）。

20 端末装置 10 のコントローラ 108 は、HD 20 から HD インターフェース部 110 およびバス BS 2 を介してクラス証明書 $Cm1$ を受理すると（ステップ S 4）、受理したクラス証明書 $Cm1$ をモデム 106 およびネットワーク 30 を介してライセンス提供装置 40 へ送信する（ステップ S 5）。

ライセンス提供装置 40 では、端末装置 10 からクラス証明書 $Cm1$ を受信すると（ステップ S 6）、受信した $Cm1$ が正当なクラス証明書であるか否かを認証する（ステップ S 7）。認証処理は次のように行なわれる。

25 ライセンス提供装置 40 は、クラス証明書 $Cm1 = KP_{cm1} // I_{cm1} // E(K_a, H(KP_{cm1} // I_{cm1}))$ を受理すると、HD 20 から出力されたクラス証明書 $Cm1$ に含まれる署名データ $E(K_a, H(KP_{cm1} // I_{cm1}))$ を認証部 418 において認証鍵 KPa で復号し、ハッシュ値 $H(KP_{cm1} // I_{cm1})$ を抽出する。そして、さらに、認証部 418 は、クラス証

明書Cm1に含まれるKPcm1//Icm1のハッシュ値を演算し、クラス証明書Cm1から抽出したハッシュ値と演算したハッシュ値とを比較する。配信制御部412は、認証部418における復号処理結果から、上記の復号ができ、かつ、2つのハッシュ値の値が一致したと判断すると、HD20から受理したクラス証明書Cm1は、正当な証明書であると判断する。

ステップS7において、クラス証明書Cm1が正当な証明書であると判断された場合、配信制御部418は、クラス公開鍵KPcm1を受理する（ステップS8）。そして、次の処理（ステップS9）へ移行する。正当なクラス証明書でない場合には、クラス証明書Cm1を受理しないでエラー通知を端末装置10へ出力し（図10のステップS44）、端末装置10においてエラー通知が受理されると（図10のステップS45）、配信セッションが終了する。

ステップS8においてクラス公開鍵KPcm1が受理されると、配信制御部412は、ライセンスID（LID）を生成し（ステップS9）、さらに制御情報ACを生成する（ステップS10）。そして、セッション鍵発生部414は、配信のためのセッション鍵Ks1aを生成する（ステップS11）。セッション鍵Ks1aは、認証部418によって得られたHD20に対応するクラス公開鍵KPcm1によって、暗号処理部420によって暗号化され、暗号データE（KPcm1, Ks1a）が生成される（ステップS12）。

そして、配信制御部412は、ライセンスID（LID）および暗号化されたセッション鍵Ks1aを1つのデータ列LID//E（KPcm1, Ks1a）として、バスBS1および通信装置450を介して端末装置10へ向けて出力する（ステップS13）。

端末装置10は、ネットワーク30を介してLID//E（KPcm1, Ks1a）を受信すると（ステップS14）、受信したLID//E（KPcm1, Ks1a）をHD20へ出力する（ステップS15）。そして、HD20のコントローラ214は、端子210およびATAインターフェース部212を介してLID//E（KPcm1, Ks1a）を受理する（ステップS16）。コントローラ214は、バスBS3を介して受理したE（KPcm1, Ks1a）を復号処理部230へ与え、復号処理部230は、Kcm保持部204に保持される

HD 20に固有なクラス秘密鍵 K_{cm1} によって復号処理することにより、セッション鍵 K_{s1a} を復号し、セッション鍵 K_{s1a} を受理する（ステップS17）。

5 HD 20のコントローラ214は、ライセンス提供装置40で生成されたセッション鍵 K_{s1a} の受理を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介して、HD 20においてセッション鍵 K_{s1a} が受理された旨の通知を受理すると、HD 20にセッション鍵の生成の要求通知をバスBS2およびHDインターフェース部
10 110を介してHD 20へ出力する（ステップS18）。HD 20のコントローラ214は、端子210およびATAコントローラ212を介してセッション鍵の生成要求通知を受理すると、セッション鍵発生部226に対してセッション鍵の生成を指示する。そして、セッション鍵発生部226は、セッション鍵 K_{s2a} を生成する（ステップS19）。

15 そして、コントローラ214は、セキュアデータ記憶部250のログメモリ253から最も古いログが格納されているバンクを検索し、その検索したバンク n ($0 \leq n \leq N-1$)の管理番号領域2541、ライセンスID領域2542、 K_{s2a} 領域2543、ST1領域2544に対して、それぞれ、新たな管理番号、ステップS16で受理したライセンスID、ステップS19において生成さ
20 れたセッション鍵 K_{s2a} 、および”受信待”を格納する（ステップS20）。したがって、バンク n に格納されるログは最も新しいログとなる。このとき、ログを構成する他の領域については、その内容を初期化、たとえば、全て”0”としてもよいし、そのままの状態であってもよい。

ここで、図11を参照して、ステップS20の詳細な動作について説明する。
25 図11は、ステップS20の詳細な動作を示すフローチャートである。、コントローラ214は、ステップS19の後、ログメモリ253のうち、最新のログが記録されているログ領域に対応するバンク $n-1$ を特定し、そのバンク $n-1$ によって指定されるログ領域に格納された履歴情報に含まれる管理番号 m を取得する（ステップS20a）。

図 1 2 を参照して、ステップ S 2 0 a の詳細な動作について説明する。図 1 2 は、ステップ S 2 0 のさらに詳細なフローチャートである。コントローラ 2 1 4 は、ステップ S 1 9 の後、変数 n に対して領域 2 5 3 2 を示すバンク 1 のバンク番号 1 を設定し（ステップ S 2 0 c）、バンク 0 に格納されている管理番号を取得して、変数 m に代入する（ステップ S 2 0 d）。そして、コントローラ 2 1 4 は、ログメモリ 2 5 3 のバンク n に格納されている管理番号を取得して、変数 m_a に代入する（ステップ S 2 0 e）、 $m_a - m$ を演算して演算結果が” 1 ” であるか否かを判定する（ステップ S 2 0 f）。演算結果が” 1 ” であるとき、コントローラ 2 1 4 は、変数 n に、1 を加えた $n + 1$ を代入し（ステップ S 2 0 g）、変数 m_a に代入されている管理番号を変数 m に代入する（ステップ S 2 0 h）。その後、ステップ S 2 0 e ~ S 2 0 h が繰返し行なわれる。

ステップ S 2 0 f において、コントローラ 2 1 4 は、演算結果が” 1 ” でないとき、バンク $n - 1$ が、最新のログが記録されている領域であると判断し、最新の管理番号 m の取得を終了し、図 1 1 に示すステップ S 2 0 b へ移行する。このとき、最も古いログはバンク n に格納されている。

ステップ S 2 0 f において、演算結果が” 1 ” であると判定された場合に、ステップ S 2 0 g, S 2 0 h, S 2 0 e, S 2 0 f が、順次、行なわれるのは、演算結果が” 1 ” である場合、変数 m と変数 m_a とに代入された管理番号 m と管理番号 m_a とが連続した番号であり、バンク $n - 1$ とバンク n とに、前後してログが格納されたことを示している。つまり、ログメモリ 2 5 3 の領域はバンク番号順に巡回的に使用され、かつ、管理番号も M の剰余系において巡回的に使用されるのであるから連続して格納された場合、連続するバンクに格納された管理番号の差は” 1 ” となるからである。したがって、バンク $n - 1$ には、最新のログが格納されていないことが判る。なお、バンク n については不明である。そして、判断する領域を 1 つ進めて、バンク n に格納されているログについて判定する。すなわち、バンク n に格納されているログの管理と、次の領域であるバンク $n + 1$ に格納されているログの管理番号に基づいて判定する。フローチャートでは、ステップ S 2 0 g において、 n には $n + 1$ が代入されることで次の領域に対する判定となる。

このように、ステップ S 2 0 f, S 2 0 g, S 2 0 h, S 2 0 e のループを繰返し行なうことによってバンク 0 から順にバンク N-1 まで連続した領域に格納された管理番号が連続しているか否かが判定される。なお、バンク N-1 と比較されるのはバンク 0 の番号である、上述したように、バンクの番号に対する演算は N の剰余系においてなされる。すなわち、バンク N-1 の判定においては、 $n-1=N-1$ 、 $n=0$ である。

ステップ S 2 0 f において、演算結果が "1" でない場合に、バンク $n-1$ に格納されたログを最新のログと判定するのは、この場合、バンク $n-1$ およびバンク n に格納される 2 つのログの管理番号が不連続であるからである。すなわち、上述したように、前後してログの管理番号は連続する。逆に連続しない管理番号を含むログは連続しないこととなる。

また、図 1 2 に従ってバンク $n-1$ を特定するためには、HD 2 0 の出荷時におけるログメモリ 2 5 3 の初期化によってログメモリ 2 5 3 の全ての領域 2 5 3 1 ~ 2 5 3 N に、すなわち、バンク 0 ~ バンク N-1 に対して、所定の管理番号を含むログを格納しておく必要がある。管理番号として全てのバンクに対して同じ値、あるいは、連続するバンクに連続する値（一ヶ所不連続となる）を持つログを格納しておく。なお、ログの他の領域については、いずれの値であってもよい。

再び、図 1 1 を参照して、上述した方法によって最新の履歴情報（ログ）が記録されているバンク $n-1$ と、バンク $n-1$ に格納された管理番号 m とを取得した後、コントローラ 2 1 4 は、バンク n に、管理番号 $m+1$ 、ステップ S 1 6 で受理したライセンス ID、ステップ S 1 9 で受理したセッション鍵 K_{s2a} を格納し、ST 1 領域 2 5 4 5 のステータス ST 1 を "受信待" に設定する（ステップ S 2 0 b）。これにより、図 9 に示すステップ S 2 0 の動作が終了し、ステップ S 2 1 へ移行する。

再び、図 9 を参照して、ステップ S 2 0 の後、暗号処理部 2 2 4 は、切換スイッチ 2 6 0 の接点 P b を介して復号処理部 2 3 0 より与えられるセッション鍵 K_{s1a} によって、切換スイッチ 2 6 2 の接点 P d と P f とを順に切換えることによって与えられるセッション鍵 K_{s2a} と個別公開鍵 K_{Pom2} とからなる 1 つ

のデータ列を暗号化し、 $E(Ks1a, Ks2a // KPom2)$ 生成する（ステップS21）。そして、暗号処理部224は、 $E(Ks1a, Ks2a // KPom2)$ をバスBS3に出力する。バスBS3に出力された暗号化データ $E(Ks1a, Ks2a // KPom2)$ は、コントローラ214により受理され、
5 コントローラ214は、受理した暗号化データとライセンスID(LID)とを1つのデータ列としたデータ $LID // E(Ks1a, Ks2a // KPom2)$ をATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS22）。

そして、端末装置10は、データ $LID // E(Ks1a, Ks2a // KPom2)$ をHD20から受理すると（ステップS23）、受理したデータをネットワーク30を介してライセンス提供装置40に出力する（ステップS24）。
10

ライセンス提供装置40は、データ $LID // E(Ks1a, Ks2a // KPom2)$ を受信すると（ステップS25）、復号処理部422においてセッション鍵 $Ks1a$ による復号処理を実行し、HD20で生成されたセッション鍵 $Ks2a$ 、およびHD20の個別公開鍵 $KPom2$ を受理する（ステップS26）。
15

配信制御部412は、ライセンスID(LID)に対応するデータID(DID)およびコンテンツ鍵 Kc をコンテンツDB402から取得し（ステップS27）、ライセンスID(LID)および制御情報ACと併せた1つのデータ列としてのライセンス $LIC = Kc // AC // DID // LID$ を生成する。

配信制御部412は、生成したライセンス LIC を暗号処理部424に与える。暗号処理部424は、復号処理部422によって得られたHD20の個別公開鍵 $KPom2$ によってライセンス LIC を暗号化して暗号化データ $E(KPom2, LIC)$ を生成する（ステップS28）。そして、暗号処理部426は、暗号処理部424から受ける暗号化データ $E(KPom2, LIC)$ を、復号処理部4
20 22から受けるセッション鍵 $Ks2a$ によって暗号化し、暗号化データ $E(Ks2a, E(KPom2, LIC))$ を生成する（ステップS29）。
25

図10を参照して、配信制御部412は、バスBS1および通信装置450を介して暗号化データ $E(Ks2a, E(KPom2, LIC))$ を端末装置10へ向けて出力する（ステップS30）。端末装置10は、ネットワーク30を介

して暗号化データE (K s 2 a, E (K P o m 2, L I C)) を受理すると (ステップS 3 1)、受理した暗号化データをHD 2 0へ出力する (ステップS 3 2)。

5 HD 2 0のコントローラ2 1 4は、端子2 1 0およびATAインターフェース部2 1 2を介して暗号化データE (K s 2 a, E (K P o m 2, L I C)) を受理すると (ステップS 3 3)、バスBS 3へ出力する。復号処理部2 2 8は、セッション鍵発生部2 2 6から与えられたセッション鍵K s 2 aを用いてバスBS 3に出力されたデータE (K s 2 a, E (K P o m 2, L I C)) を復号し、HD 2 0において、ライセンスL I Cが個別公開鍵K P o m 2により暗号化された暗号化ライセンスE (K P o m 2, L I C) が受理される (ステップS 3 4)。
10 そして、復号処理部2 2 8は、暗号化ライセンスE (K P o m 2, L I C) をバスBS 3へ出力する。

コントローラ2 1 4の指示によって、暗号化ライセンスE (K P o m 2, L I C) は、復号処理部2 1 6において個別秘密鍵K o m 2によって復号され、ライセンスL I Cが受理される (ステップS 3 5)。
15

HD 2 0のコントローラ2 1 4は、ライセンスL I Cの受理を確認すると、ATAインターフェース部2 1 2および端子2 1 0を介してその旨を端末装置1 0に通知する。端末装置1 0のコントローラ1 0 8は、HDインターフェース部1 1 0およびバスBS 2を介して、HD 2 0においてライセンスL I Cが受理された旨の通知を受理すると、HD 2 0のセキュアデータ記憶部2 5 0において、その受信したライセンスL I Cを格納するLBA (「格納LBA」と呼ぶ。) をバスBS 2およびHDインターフェース1 1 0を介してHD 2 0へ出力する (ステップS 3 6)。
20 HD 2 0のコントローラ2 1 4は、端子2 1 0およびATAインターフェース部2 1 2を介してライセンスL I Cの格納LBAを受理すると (ステップS 3 7)、その受理した格納LBAをログメモリ2 5 3のバンクnに格納されたログのLBA領域2 5 4 7に記憶する (ステップS 3 8)。
25

そして、コントローラ2 1 4は、受理したライセンスL I Cに含まれるライセンスID (L I D) と、ステップS 1 6において受理したライセンスL I D (L I D) とを比較し、一致しているか否かをチェックする (ステップS 3 9)。コ

ントローラ 214 は、L I D が一致しており、受理したライセンス L I C が正しいものであると判断すると、端末装置 10 から受理したセキュアデータ記憶部 250 内の L B A に、受理したライセンス L I C を記憶する（ステップ S 40）。

5 コントローラ 214 は、指定された L B A にライセンス L I C を記憶すると、有効フラグ領域 252 のその L B A に対応するフラグを”有効”にする（ステップ S 41）。そして、コントローラ 214 は、さらに、ログメモリ 253 のバンク n に格納されたログの S T 1 領域 2544 のステータス S T 1 を”受信済”に変更し（ステップ S 42）、配信セッションにおける一連の処理が終了したことを端末装置 10 に通知する。

10 そして、端末装置 10 において、H D 20 から処理終了通知が受理されると、データ配信システムにおける配信セッションが正常終了する。

一方、ステップ S 39 において、コントローラ 214 は、L I D が一致せず、受理したライセンス L I C が正しくないと判断すると、エラー通知を端末装置 10 へ出力し（ステップ S 43）、端末装置 10 は、エラー通知を受理すると（ステップ S 45）、処理を終了する。

15 図 9 および図 10 に示された配信処理においては、ライセンス提供装置 40 におけるログの記録に関する記載がなされていないが、図 4 に示すように、ライセンス提供装置 40 には、十分な記憶容量を持つログ D B 404 が備えられており、配信セッションにおける各ステップにおけるログがログ D B 404 に記憶される。また、ログ D B 404 には、ライセンスの送信に伴う課金情報なども記憶される。

20 図 9 および図 10 に示された配信処理における一連の処理において、ステップ S 25 からステップ S 44 の処理中に異常が発生して処理が中断したときは、再書込処理の対象となる。たとえば、中断の理由として、上記処理中に端末装置 10 の電源が遮断されたり、ライセンス提供装置 40 側の異常、あるいは端末装置 10 とライセンス提供装置 40 との通信異常など、種々の異常ケースが考えられる。ここで、H D 20 内のログメモリ 253 に格納されたステータス S T 2 を除く出力ログの内容がすべて格納されたステップ S 22 終了後からステップ S 44 までの処理中に処理が中断した場合には、H D 20 は、再書込処理を行なってラ

イセンスの提供を受けることが可能である。ここでは、端末装置 10 の判断によって再書込処理を行なうものとしたため、端末装置 10 において処理の進行が確認できるステップ S 2 2 からステップ S 2 4 を除く、ステップ S 2 5 からステップ S 4 4 の処理中に処理が中断した場合を再書込処理の対象とし、他のステップ
5 における処理の中断においてはライセンス提供装置 40 からライセンスの提供がなされなかったものと判断し、図 9 および図 10 に示したフローチャートに従って、最初から処理を行なうこととした。

同様に、ライセンス提供装置 40 がライセンスを出力するまでのライセンス提供装置 40 内のステップ S 2 5 からステップ S 3 0 までの処理については、端末
10 装置 10 において、これらのいずれのステップを処理中に処理が中断したかを特定できる場合には、再書込処理の対象から除外して、図 9 および図 10 に示したフローチャートにしたがって、最初から処理を行なうものとしてもよい。

〔配信における再書込〕

図 1 3 ～図 1 5 は、図 9 および図 10 において示した配信処理におけるステップ S 2 5 からステップ S 4 4 の処理中に異常が発生したときに行なわれる再書込
15 処理の第 1 から第 3 のフローチャートであり、図 1 6 は、図 1 3 のステップ S 1 1 2 a の詳細な動作を説明するためのフローチャートである。

図 1 3 を参照して、端末装置 10 は、ステップ S 2 5 からステップ S 4 4 の処理中に異常が発生したと判断すると、ライセンス L I C の L I D / / 再書込要求
20 をネットワーク 30 を介してライセンス提供装置 40 へ出力する（ステップ S 1 0 1）。配信制御部 4 1 2 は、通信装置 4 5 0 およびバス B S 1 を介して L I D / / 再書込要求を受理すると（ステップ S 1 0 2）、セッション鍵発生部 4 1 4 にセッション鍵を生成するように指示する。指示を受けたセッション鍵発生部 4 1 4 は、再書込処理のためのセッションキー鍵 K s 1 b を生成する（ステップ S
25 1 0 3）。そして、配信制御部 4 1 2 は、このセッションにおいて H D 2 0 とやり取りしたログが格納されているログ D B 4 0 2 から H D 2 0 に対応するクラス公開鍵 K P c m 1 を取得し（ステップ S 1 0 4）、暗号処理部 4 2 0 に与える。クラス公開鍵 K P c m 1 を受けた暗号処理部 4 2 0 は、クラス公開鍵 K P c m 1 をによりセッション鍵 K s 1 b を暗号化し、E (K P c m 1, K s 1 b) が生成

される（ステップS105）。そして、配信制御部412は、LID//E（K P c m 1, K s 1 b）をバスBS1および通信装置450を介して端末装置10へ向けて出力する（ステップS106）。

5 端末装置10は、ネットワーク30を介してLID//E（K P c m 1, K s 1 b）を受理すると（ステップS107）、受理したLID//E（K P c m 1, K s 1 b）をHD20へ出力する（ステップS108）。そして、HD20のコントローラ214は、端子210およびATAインターフェース部212を介してLID//E（K P c m 1, K s 1 b）を受理する（ステップS109）。コントローラ214は、受理したE（K P c m 1, K s 1 b）をバスBS3を介して復号処理部230へ与え、復号処理部230は、K c m保持部204に保持されるHD20に固有なクラス秘密鍵K c m 1によって復号処理することにより、セッション鍵K s 1 bを復号し、セッション鍵K s 1 bが受理される（ステップS110）。

15 HD20のコントローラ214は、ライセンス提供装置40で生成されたセッション鍵K s 1 bの受理を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介して、HD20においてセッション鍵K s 1 bが受理された旨の通知を受理すると、ログの出力要求をバスBS2およびHDインターフェース部110を介してHD20へ出力する（ステップS111）。

20 HD20のコントローラ214は、端子210およびATAコントローラ212を介してログの出力要求通知を受理し（ステップS112）、ログの複製処理を行なう（ステップS112a）。

25 ここで、図16を参照して、ステップS112aの詳細な動作について説明する。コントローラ214は、ログメモリ253のうち、最新のログが格納されたバンクn-1の特定と、バンクn-1に格納されているログの管理番号mとを取得する（ステップS112b）。このステップS112bの詳細な動作は、図11および図12に示すフローチャートに従って行なわれる。

ステップS112bの後、コントローラ214は、変数k（kは自然数、 $1 \leq$

$k \leq N$) に” 1 ” を、変数ERRに” 偽 ” を代入し (ステップS 1 1 2 c)、バンク $n - k$ に格納されたログのライセンスID (LID) が、ステップS 1 0 9 で受理したライセンスID (LID) に一致するか否かを判定する。すなわち、コントローラ 2 1 4 は、ステップS 1 1 2 b で検出した最新のログに格納された

5 ライセンスID (LID) が、ステップS 1 0 9 で受理したライセンスID (LID) に一致するか否かを判定する。

2つのライセンスID (LID) が不一致である場合、コントローラ 2 1 4 は、 k が N (バンクの総数) よりも小さいか否かを判定し (ステップS 1 1 2 e)、 k が N 以上であるとき、全てのバンクに対して確認が終了し、つまり、受理した

10 ライセンスID (LID) に一致するLIDを記録したログが格納されていないことが確認され、ステップS 1 1 2 h へ進み、変数ERRに” 真 ” を代入する (ステップS 1 1 2 h)。そして、図 1 3 のステップS 1 1 3 a に戻り、変数ERRを確認する。

再び、図 1 3 を参照して、コントローラ 2 1 4 は、変数ERRを確認する (ステップS 1 1 3 a)。図 1 6 のステップS 1 1 2 h から移行した場合、変数ERRは” 真 ” であり、該当するライセンスIDを記録するログが、ログメモリ 2 5 3 に格納されていなかったことを示しているので処理を継続することはできない。したがって、図 1 5 に示すステップS 1 6 0 へ移行し、エラー通知を端末装置 1 0 へ出力する (ステップS 1 6 0)。そして、端末装置 1 0 は、エラー通知を受

15 理し (ステップS 1 6 1)、書込拒否により一連の動作が終了する。

図 1 6 を参照して、ステップS 1 1 2 e において、コントローラ 2 1 4 は、 k は N よりも小さいと判定すると、全てのバンクに対する確認が終了していないので、今、確認したログより、1つ古いログを確認するために、変数 k に $k - 1$ を代入する (ステップS 1 1 2 f)、ステップS 1 1 2 d へ移行する。そして、コ

25 ントローラ 2 1 4 は、バンク $n - k$ に格納されたライセンスID (LID) が、ステップS 1 0 9 で受理したライセンスID (LID) と一致するか否かを判定する。この場合、変数 k の値は” 2 ” であるので、コントローラ 2 1 4 は、バンク $n - 2$ に格納されたログのライセンスID (LID) が、ステップS 1 0 9 で受理したライセンスID (LID) に一致するか否かを判定する。そして、2つ

のライセンスID (LID) が不一致である場合、ステップS112e, S112f, S112dが行なわれる。

このように、コントローラ214は、最新のログから、より古いログが格納されるバンクへ向けて、各バンクに格納されたライセンスID (LID) が、ステップS109で受理したライセンスID (LID) と一致するか否かを判定する。そして、この動作 (ステップS112e, S112f, S112d) は、ステップS109で受理したライセンスID (LID) に一致するライセンスID (LID) が検出されるまで、あるいは、全てのバンクの確認が終了するまで繰返し行なわれる。なお、バンク番号はNの剰余系であるので、ライセンスIDの確認は、バンク $n-1$ ($k=1$), $n-2$ ($k=2$), \dots , 1 ($k=n-1$), 0 ($k=n$), $N-1$ ($k=n+1$), \dots , n ($k=N$) の順に確認される。

ステップS112dにおいて、2つのライセンスID (LID) が一致したとき、コントローラ214は、バンク $n-k$ に格納されたログを取得し、その取得したログの管理番号 m を $m+1$ に変更した後、そのログをバンク n に格納する (ステップS112g)。つまり、コントローラ214は、ライセンス提供装置40から送信されたライセンスID (LID) に一致するライセンスID (LID) を含むログがログメモリ253に格納されている場合、そのログ (複数有る場合は、より新しいログ) を、最も古いログが格納されたバンク n に複製する。この場合、管理番号のみは複製されず、複製したログが新しいログとして扱われるよう先のバンク $n-1$ に格納されたログの管理番号に1を加えた値を記録する。したがって、最も古いログは削除され、そこに、現在、進行中の再書込処理に対する新たなログが格納される。

その後、図13に示すステップS113aへ移行する。

再び、図13を参照して、コントローラ214は、変数ERRを格納する (ステップS133a)。図16に示すステップS112gから移行した場合、変数ERRは”偽”であり、該当するライセンスIDを記録したログがバンク n に複製されるので処理の継続が可能であると判断され、ステップS113へ移行して、ログメモリ253のバンク n に格納された格納LBAに記憶されるライセンスLICのライセンスID (LID) と、ログメモリ253に格納されたライセンス

ID (LID) とが一致するか否かをチェックする (ステップ S 1 1 3)。

コントローラ 2 1 4 は、両ライセンス ID (LID) が一致すると判断すると、配信処理としては、ライセンス提供装置 4 0 からのライセンス LIC の受理までは行なわれ、HD 2 0 においてライセンス LIC は受理していると認識する。そうすると、コントローラ 2 1 4 は、ログメモリ 2 5 3 のバンク n に格納された格納 LBA により指定された領域に記憶されるライセンスに対応する有効フラグ領域 2 5 2 に格納されているフラグをチェックして、そのライセンスの有効性をチェックする (ステップ S 1 1 4)。

コントローラ 2 1 4 は、ライセンスが有効であると判断すると、ログメモリ 2 5 3 のバンク n に格納されたログのステータス ST 2 を” データ有” に変更し、次の処理 (ステップ S 1 1 8) へ移行する。一方、コントローラ 2 1 4 は、ステップ S 1 1 4 においてライセンスが無効であると判断すると、ログメモリ 2 5 3 のバンク n に格納されたログのステータス ST 2 を” 移動済” に変更し、次の処理 (ステップ S 1 1 8) へ移行する。

ステップ 1 1 3 において、コントローラ 2 1 4 は、比較したライセンス ID (LID) が一致しないと判断したときは、ログメモリ 2 5 3 のバンク n に格納されたログのステータス ST 2 を” データ無” に変更する (ステップ S 1 1 7)。

ステータス ST 2 の変更処理がなされると、コントローラ 2 1 4 は、ログメモリ 2 5 3 のバンク n からライセンス ID (LID)、ステータス ST 1, ST 2 およびセッション鍵 K s 2 c を取得する (ステップ S 1 1 8)。ここで、この処理は図 9 および図 1 0 のフローチャートに従って配信セッションの中断に対する処理であるためログメモリ 2 5 3 のバンク n に格納されているセッション鍵は K s 2 a であるが、説明の関係上、ログメモリ 2 5 3 のバンク n から取得したセッション鍵を K s 2 c としている。そして、コントローラ 2 1 4 は、取得したセッション鍵 K s 2 c をバス BS 3 を介して暗号処理部 2 2 4 へ出力する。

暗号処理部 2 2 4 は、切換スイッチ 2 6 0 の接点 P b を介して復号処理部 2 3 0 より与えられるセッション鍵 K s 1 b によって、バス BS 3 から取得したセッション鍵 K s 2 c を暗号化し、E (K s 1 b, K s 2 c) 生成する (ステップ S 1 1 9)。そして、暗号処理部 2 2 4 は、生成した E (K s 1 b, K s 2 c) を

バスBS3に出力する。バスBS3に出力されたE(Ks1b, Ks2c)は、コントローラ214により受理され、コントローラ214は、ステップS118において取得したデータとともに1つのデータ列LID//E(Ks1b, Ks2c)//ST1//ST2を生成し、ハッシュ関数を用いてハッシュ値H(LID//E(Ks1b, Ks2c)//ST1//ST2)を生成する(ステップS120)。そして、コントローラ214は、ハッシュ値H(LID//E(Ks1b, Ks2c)//ST1//ST2)をバスBS3を介して暗号処理部224へ出力する。

暗号処理部224は、切換スイッチ260の接点Pbを介して復号処理部230より与えられるセッション鍵Ks1bによって、バスBS3から取得したハッシュ値H(LID//E(Ks1b, Ks2c)//ST1//ST2)を暗号化し、E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))を生成する(ステップS121)。そして、暗号処理部224は、生成したE(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))をバスBS3に出力する。ここで、データ列LID//E(Ks1b, Ks2c)//ST1//ST2を受信ログと称し、E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))は、受信ログに対してセッション鍵Ks1bを用いて電子署名を行なった署名データである。また、ログメモリ253に格納されていたセッション鍵Ks2cをセッション鍵Ks1bを用いて暗号化するのは、セッション鍵Ks2cの漏洩によるライセンスの流出の危険性を排除するためである。

コントローラ214は、バスBS3から署名データを受理すると、ステップS118において取得した受信ログを用いて、署名付き受信ログLID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))を生成し、ATAインターフェース部212および端子210を介して端末装置10へ出力する(ステップS122)。

端末装置10は、署名付き受信ログLID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)))

／／ST1／／ST2))をHD20から受理すると(ステップS123)、受理したデータをネットワーク30を介してライセンス提供装置40へ出力する(ステップS124)。そして、ライセンス提供装置40は、ネットワーク30を介して署名付き受信ログLID／／E(Ks1b, Ks2c)／／ST1／／ST2／／E(Ks1b, H(LID／／E(Ks1b, Ks2c)／／ST1／／ST2))を受信する。(ステップS125)

図14を参照して、ライセンス提供装置40は、受信した署名付き受信ログLID／／E(Ks1b, Ks2c)／／ST1／／ST2／／E(Ks1b, H(LID／／E(Ks1b, Ks2c)／／ST1／／ST2))の検証を行なう(ステップS126)。検証処理は次のように行なわれる。

配信制御部412は、署名付き受信ログを受理すると、まず、受理した署名付き受信ログの後半部である署名データE(Ks1b, H(LID／／E(Ks1b, Ks2c)／／ST1／／ST2))を復号処理部422へ出力するとともに、セッション鍵発生部414にセッション鍵Ks1bを発生するように指示する。そして、復号処理部422は、セッション鍵Ks1bによって署名データE(Ks1b, H(LID／／E(Ks1b, Ks2c)／／ST1／／ST2))を復号し、HD20にて演算したハッシュ値を抽出する。一方、配信制御部412は、署名付き受信ログの前半部である受信ログLID／／E(Ks1b, Ks2c)／／ST1／／ST2のハッシュ値を演算し、復号処理部422により復号されたHD20で演算されたハッシュ値と比較する。配信制御部412は、2つのハッシュ値が一致したと判断すると、HD20から受理したデータ列は、正当なデータを含むものとしてライセンス提供装置40において承認される。

ステップS126においてHD20から受理した署名付き受信ログが承認されると、配信制御部412は、受理したライセンスID(LID)に基づいてログDB404を検索する(ステップS127)。配信制御部412は、受理したライセンスID(LID)がログDB404内に格納されており、HD20に対して確かに提供を行なったライセンスであると判断すると、受理したステータスST1, ST2の内容を確認する(ステップS128)。

配信制御部412は、ステータスST1が”受信待”であり、ステータスST

2が”データ無”であるとき、HD 20に送信したはずのライセンスLICが何らかの異常によりHD 20において受理されていないと判断し、受信したデータ列に含まれる暗号化データE (K s 1 b, K s 2 c)を復号処理部422へ出力してセッション鍵K s 1 bによってセッション鍵K s 2 cを復号する。そして、
5 復号されたセッション鍵K s 2 cは、バスBS1を介して配信制御部412へ出力され、配信制御部412においてセッション鍵K s 2 cが受理される（ステップS129）。

そして、配信制御部412は、異常発生時のセッション鍵K s 2 aを今回受理したセッション鍵K s 2 cと比較チェックする（ステップS130）。配信制御部412は、セッション鍵K s 2 aとセッション鍵K s 2 cとが一致していると
10 判断すると、ライセンスLICの再書込に対する許可通知を端末装置10へ出力する（ステップS133）。

一方、ステップS126においてHD 20から受理したデータ列が承認されなかったとき、ステップS127においてHD 20から受理したライセンスID (LID)がログDB404内に格納されておらず、HD 20に対して提供を行
15 なったライセンスであると判断できないとき、ステップS128において、HD 20においてライセンスLICが受理されたものと判断されたとき、またはステップS130において、セッション鍵K s 2 aがセッション鍵K s 2 cと一致しないと判断されたときは、配信制御部412は、ライセンスの再送信は不可と判
20 断し、バスBS1および通信装置450を介してエラー通知を端末装置10へ向けて出力し（ステップS131）、端末装置10は、ネットワーク30を介してエラー通知を受理すると（ステップS132）、処理が終了する。すなわち、ライセンス提供装置40において、ライセンスの再書込が拒否されて処理が終了する。

25 端末装置10のコントローラ108は、ステップS133においてライセンス提供装置40が出力した許可通知を受理すると（ステップS134）、HD 20に対するセッション鍵の生成の要求通知をバスBS2およびHDインターフェース部110を介してHD 20へ出力する（ステップS135）。

HD 20は、ライセンス提供装置40からの再書込処理許可通知に基づいて、

端末装置 10 からセッション鍵の生成要求通知を受理すると、新たにセッション
鍵 K_{s2b} を生成し（ステップ $S136$ ）、ログメモリ 253 のバンク n のログ
に記録されているセッション鍵 K_{s2c} （= K_{s2a} ）を、生成したセッション
鍵 K_{s2b} に、ログのステータス $ST1$ を”受信待”に変更する（ステップ $S1$
5 37）。

以下、ステップ $S138$ からの一連の処理は、図 9 および図 10 において説明
したステップ $S21$ から処理終了までの一連の処理において、セッション K_{s2}
 a に代えて新たに生成してセッション鍵 K_{s2b} が使用される他は、同様の処理
が行なわれる。したがって、ステップ $S138$ からの一連の処理の説明は繰返し
10 になるので省略する。

なお、図 13～図 15 のフローチャートに示されるライセンスの配信における
再書込処理中の中断に対しては、ステップ $S101$ ～ $S131$ 、ステップ $S13$
3 およびステップ $S142$ ～ $S160$ のいずれかのステップにおいて処理が中断
した場合には、再び図 13～図 15 のフローチャートに従って再書込処理を行な
15 うことができる。一方、ステップ $S134$ ～ $S141$ のいずれかのステップにお
いて処理が中断した場合には、図 9 および図 10 のフローチャートに示されるラ
イセンスの配信処理を最初から行なうことによって、処理を再開することができ
る。

このようにして、端末装置 10 に装着された $HD20$ が正規のクラス証明書 C
20 $m1$ を保持する機器であることを確認したうえで、クラス証明書 C_{m1} に含まれ
て送信されたクラス公開鍵 $K_{P_{cm1}}$ によってライセンス提供装置 40 および H
 $D20$ でそれぞれ生成される暗号鍵（セッション鍵）をやり取りし、お互いが受
領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信する
ことによって、それぞれの暗号化データの送受信においても事実上の相互認証を
25 行なうことができる。これによって、不正なハードディスクへのライセンスの配
信を禁止することができ、データ配信システムのセキュリティを向上させること
ができる。

さらに、ライセンスの配信処理が中断しても、受信側のデータ記憶装置である
 $HD20$ における署名付き受信ログをライセンス提供装置 40 へ送信することで、

ライセンスの重複配信を行なうことなく、ライセンスの再送処理を安全に行なうことができる。

〔複製・移動〕

図17は、ライセンスの複製・移動が行なわれるシステムの構成を概念的に示した概略図である。図17を参照して、端末装置10にデータ記憶装置として2台のHD20、21が装着可能であり、端末装置10を介してHD20からHD21へライセンスの複製または移動が行なわれる。

ここで、HD21は、HD20と異なるデータ記憶装置であるため、HD20とは異なる個別公開鍵 KP_{om5} と個別秘密鍵 K_{om5} とを保持している。この場合、HD21における識別子 z は、HD20の $z=2$ とは異なる $z=5$ となる。また、HD21のクラスは、HD20のクラスと同じ $y=1$ として以下説明する。すなわち、HD20、HD21とも、クラス証明書 $C_{m1} = KP_{cm1} // I_{cm1} // E(K_a, KP_{cm1} // I_{cm1})$ およびクラス秘密鍵 K_{cm1} を保持する。しかしながら、HD21のクラスがHD20のクラスと異なる($y \neq 1$)場合には、クラス証明書およびクラス秘密鍵も、個別公開鍵および個別秘密鍵と同様に、HD20とは異なったものとなる。

図18および図19は、図17に示すライセンスの複製・移動が可能なシステムにおいて、端末装置10のユーザが端末装置10から暗号化コンテンツデータのライセンスの複製または移動のリクエストを行なうことにより、端末装置10を介して端末装置10に装着されたHD20からHD21へライセンスの複製または移動が行なわれる際の処理(複製・移動セッション)を説明するための第1および第2のフローチャートである。

図18を参照して、端末装置10のユーザから所望のコンテンツデータのライセンスに対する複製または移動の要求が発せられると、端末装置10のコントローラ108は、バスBS2およびHDインターフェース部110を介してHD21へクラス証明書の出力要求を出力する(ステップS201)。HD21においては、端子210およびATAインターフェース部212を介してクラス証明書の出力要求が受理されると(ステップS202)、コントローラ214は、認証データ保持部202からクラス証明書 $C_{m1} = KP_{cm1} // I_{cm1} // E$

(K a, H (K P c m 1 / / I c m 1)) を読出し、クラス証明書C m 1をA T Aインターフェース部2 1 2および端子2 1 0を介して端末装置1 0へ出力する(ステップS 2 0 3)。

5 端末装置1 0は、HD 2 1からクラス証明書C m 1を受理すると(ステップS 2 0 4)、受理したクラス証明書C m 1をHD 2 0へ送信する(ステップS 2 0 5)。

HD 2 0では、端末装置1 0からHD 2 1のクラス証明書C m 1を受理すると(ステップS 2 0 6)、認証部2 2 0およびコントローラ2 1 4によって受理したHD 2 1のクラス証明書C m 1が正当なクラス証明書であるか否かを認証する(ステップS 2 0 7)。認証処理は、ライセンス提供装置4 0における認証処理(図9のステップS 7)と同一であるため詳細な説明は省略する。

10 ステップS 2 0 7において、コントローラ2 1 4は、正当なHD 2 1のクラス証明書でないと判定した場合には、HD 2 1のクラス証明書C m 1を非承認として受理せず、エラー通知を端末装置1 0へ出力する(図1 9のステップS 2 5 2)。そして、端末装置1 0においてエラー通知が受理されると(図1 5のステップS 2 5 3)、配信セッションが終了する。

20 ステップS 2 0 7において、HD 2 1のクラス証明書C m 1が正当な証明書であると判断されると、HD 2 0のコントローラ2 1 4は、HD 2 1のクラス証明書C m 1を承認し、セッション鍵K s 1 aを生成するようにセッション鍵発生部2 2 6を制御し、セッション鍵発生部2 2 6は、セッション鍵K s 1 aを生成する(ステップS 2 0 9)。

セッション鍵K s 1 aは、認証部2 2 0によって得られたHD 2 1のクラス公開鍵K P c m 1によって、暗号処理部2 2 2において暗号化され、暗号化データE (K P c m 1, K s 1 a)が生成される(ステップS 2 1 0)。

25 そして、コントローラ2 1 4は、暗号化データE (K P c m 1, K s 1 a)を、A T Aインターフェース部2 1 2および端子2 1 0を介して端末装置1 0へ出力する(ステップS 2 1 1)。

端末装置1 0は、暗号化データE (K P c m 1, K s 1 a)を受理すると(ステップS 2 1 2)、受理した暗号化データE (K P c m 1, K s 1 a)をHD 2

1へ出力する（ステップS213）。ここで、ライセンスID（LID）は、事前に管理ファイルを参照することで端末装置10が取得している。管理ファイルは、HD20に記憶されている暗号化コンテンツデータとライセンスとの関係进行管理するための管理データを記録したデータファイルであって、ノーマルデータ記憶部270に記憶され、暗号化コンテンツデータの記録消去や、ライセンスの書込、移動および消去によってその内容が更新される。

そして、HD21においては、コントローラ214が、端子210およびATAインターフェース部212を介してLID//E（KPCm1, Ks1a）を受理する（ステップS214）。続いて、コントローラ214は、バスBS3を介してE（KPCm1, Ks1a）を復号処理部230へ与え、復号処理部230は、Kcm保持部204に保持されるHD21に固有なクラス秘密鍵Kcm1によって復号処理することにより、セッション鍵Ks1aを復号し、セッション鍵Ks1aを受理する（ステップS215）。

HD21のコントローラ214は、HD20で生成されたセッション鍵Ks1aの受理を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10は、HD21においてセッション鍵Ks1aが受理された旨の通知を受理すると、セッション鍵の生成の要求通知をHD21へ出力する（ステップS216）。HD21のコントローラ214は、端子210およびATAコントローラ212を介してセッション鍵の生成要求通知を受理すると、セッション鍵発生部226に対してセッション鍵の生成を指示する。そして、セッション鍵発生部226は、セッション鍵Ks2aを生成する（ステップS217）。

セッション鍵発生部226は、セッション鍵Ks2aを生成すると、バスBS3を介してコントローラ214へ出力し、コントローラ214は、セッション鍵Ks2aを受ける。そして、コントローラ214は、最も古いログを格納したバンクを検索し、そこに処理中のセッションに対するログを新たに格納する（ステップS218）。ステップS218の詳細な動作は、図11および図12に示すフローチャートに従って行なわれる。ただし、HD21における処理と、HD20における同様の処理結果を区別するために最も古いログを格納したバンクは、

バンク n_a であるとする。すなわち、図 1.1 および図 1.2 に示すフローチャートにおける変数 n を変数 n_a と読替えればよい。

したがって、ログメモリ 253 のバンク n_a に、バンク $n_a - 1$ に格納されるログの管理番号に 1 を加えた新しい管理番号と、ステップ S 214 において受理したライセンス ID (LID) とセッション鍵 K_{s2a} とを格納し、ステータス ST1 を”受信待”にする。

続いて、HD 21 においては、続いて、暗号処理部 224 は、切換スイッチ 260 の接点 P_b を介して復号処理部 230 より与えられるセッション鍵 K_{s1a} によって、切換スイッチ 262 の接点 P_d と P_f とを順に切換えることによって与えられるセッション鍵 K_{s2a} と個別公開鍵 K_{Pom5} とからなる 1 つのデータ列を暗号化し、 $E(K_{s1a}, K_{s2a} // K_{Pom5})$ を生成する (ステップ S 219)。そして、暗号処理部 224 は、 $E(K_{s1a}, K_{s2a} // K_{Pom5})$ をバス BS3 に出力する。バス BS3 に出力された暗号化データ $E(K_{s1a}, K_{s2a} // K_{Pom5})$ は、コントローラ 214 により受理され、コントローラ 214 は、受理した暗号化データとライセンス ID (LID) とを 1 つのデータ列としたデータ $LID // E(K_{s1a}, K_{s2a} // K_{Pom5})$ を ATA インターフェース部 212 および端子 210 を介して端末装置 10 へ出力する (ステップ S 220)。

そして、端末装置 10 は、データ $LID // E(K_{s1a}, K_{s2a} // K_{Pom5})$ を HD 21 から受理すると (ステップ S 221)、受理したデータを HD 20 へ出力する (ステップ S 222)。

HD 20 では、端子 210 および ATA インタフェース部 110 を介してデータ $LID // E(K_{s1a}, K_{s2a} // K_{Pom5})$ を受理すると (ステップ S 223)、復号処理部 228 においてセッション鍵 K_{s1a} による復号処理を実行し、HD 21 で生成されたセッション鍵 K_{s2a} 、および HD 21 の個別公開鍵 K_{Pom5} を抽出して受理する (ステップ S 224)。そして、復号処理部 228 は、復号したセッション鍵 K_{s2a} をバス BS3 を介してコントローラ 214 へ出力し、コントローラ 214 は、セッション鍵 K_{s2a} を受ける。そして、コントローラ 214 は、最も古いログを格納したバンクに、処理中のセッション

に対するログを新たに格納する（ステップS 2 2 5）。ステップS 2 2 5の詳細な動作は、図20に示すフローチャートに従って行なわれる。図20を参照して、ステップS 2 2 5は、ログメモリ253の最新ログが記録されたバンクn-1を特定し、かつ、バンクn-1に格納された管理番号mを取得するステップS 2 2 5 aと、バンクnに、管理番号m+1、ライセンスID（LID）、セッション鍵K s 2 a、およびクラス公開鍵K P c m yを格納し、かつ、ステータス領域を“送信待”に設定するステップS 2 2 5 bとから成る。そして、ステップS 2 2 5 aの詳細な動作は、図12に示すフローチャートに従って行なわれる。したがって、コントローラ214は、図20および図12に示すフローチャートに従って、ステップS 2 2 3において受理したライセンスID（LID）とステップS 2 2 4で受理したセッション鍵K s 2 aとをバンクnに格納し、ステータスST 1を“送信待”にする。

HD 2 0では、ステップS 2 2 5の処理を終えると、HD 2 0のコントローラ214は、その旨をATAインターフェース部212および端子210を介して端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部110およびバスBS 2を介して、HD 2 0からの通知を受理すると、HD 2 0のセキュアデータ記憶部250において、HD 2 0からHD 2 1へ送信するライセンスLICが格納されているLBA（格納LBA）をバスBS 2およびHDインターフェース110を介してHD 2 0へ出力する（ステップS 2 2 6）。HD 2 0のコントローラ214は、端子210およびATAインターフェース部212を介して送信対象のライセンスLICの格納LBAを受理すると（ステップS 2 2 7）、その受理した格納LBAをセキュアデータ記憶部250のログメモリ253のバンクnに記憶する（ステップS 2 2 8）。

そして、コントローラ214は、受理した格納LBAに格納されるライセンスLICに対応する有効フラグ領域252のフラグが“有効”であるか“無効”であるかを確認する（ステップS 2 2 9）。コントローラ214は、有効フラグが“有効”であると、格納LBAに格納されているライセンスLICを取得する（ステップS 2 3 0）。

図19を参照して、HD 2 0では、コントローラ214が、対象のライセンス

L I Cを取得すると、ライセンスL I Cに含まれるライセンスID (L I D) と、ステップS 2 2 3において受理し、ログメモリ 2 5 3のバンク n aに格納されているログに記憶されているライセンスID (L I D) とを比較し、一致しているか否かをチェックする (ステップS 2 3 1)。コントローラ 2 1 4は、一致している
5 10と判断すると、取得したライセンスL I Cに含まれる制御情報A Cを確認して利用制限がかけられていないかをチェックする (ステップS 2 3 2)。

コントローラ 2 1 4は、制御情報A CにおいてライセンスL I Cの利用が禁止されていないことを確認すると、取得したライセンスL I Cを暗号処理部 2 3 2に与える。暗号処理部 2 3 2は、復号処理部 2 2 8によって得られたHD 2 1の個別公開鍵K P o m 5によってライセンスL I Cを暗号化して暗号化データE
10 (K P o m 5, L I C) を生成する (ステップS 2 3 3)。そして、暗号処理部 2 3 2は、暗号化データE (K P o m 5, L I C) を切替スイッチP cを介して暗号処理部 2 2 4へ出力し、暗号処理部 2 2 4は、暗号処理部 2 3 2から受けた暗号化データを復号処理部 2 2 8から受けたセッション鍵K s 2 aによって暗号
15 化し、暗号化データE (K s 2 a, E (K P o m 5, L I C)) を生成する (ステップS 2 3 4)。

続いて、コントローラ 2 1 4は、対象のライセンスL I Cに含まれる制御情報A Cに基づいて、HD 2 0からHD 2 1へのライセンスL I Cの送信が「移動」であるか「複製」であるかを確認する (ステップS 2 3 5)。コントローラ 2 1
20 4は、「移動」であると確認したときは、その対象のライセンスL I Cに対応する、すなわち、格納L B Aに対応する有効フラグ領域 2 5 2のフラグを“無効”に変更する (ステップS 2 3 6)。一方、コントローラ 2 1 4は、「複製」であると確認したときには、当該ライセンスL I CがHD 2 0に残っていてもよいので、有効フラグ領域 2 5 2のフラグの変更は行なわずに次の処理 (ステップS 2
25 3 7) へ移行する。

コントローラ 2 1 4は、有効フラグ領域 2 5 2の処理が終わると、ログメモリ 2 5 3のバンク nに格納されているログのステータスS T 1を“送信済”に変更し (ステップS 2 3 7)、A T Aインターフェース部 2 1 2および端子 2 1 0を介して暗号化データE (K s 2 a, E (K P o m 5, L I C)) を端末装置 1 0

へ送信する（ステップS 2 3 8）。

一方、ステップS 2 2 9において受理した格納L B Aに対応する有効フラグ領域2 5 2のフラグが“無効”であったとき、ステップS 2 3 1においてライセンスI D（L I D）が一致しないとき、または、ステップS 2 3 2において、取得したライセンスL I Cに含まれる制御情報A Cにより当該ライセンスL I Cの利用が禁止されているときは、コントローラ2 1 4は、端末装置1 0に対してエラー通知を出力し（ステップS 2 5 2）、端末装置1 0においてエラー通知が受理されると（ステップS 2 5 3）、処理が終了する。

端末装置1 0は、ステップS 2 3 8においてHD 2 0から出力された暗号化データE（K s 2 a，E（K P o m 5，L I C））を受理すると（ステップS 2 3 9）、受理した暗号化データをHD 2 1へ出力する（ステップS 2 4 0）。

HD 2 1では、コントローラ2 1 4が、端子2 1 0およびATAインターフェース部2 1 2を介して暗号化データE（K s 2 a，E（K P o m 5，L I C））を受理し（ステップS 2 4 1）、バスB S 3へ出力する。復号処理部2 2 8は、セッション鍵発生部2 2 6から与えられたセッション鍵K s 2 aを用いてバスB S 3に出力されたデータE（K s 2 a，E（K P o m 5，L I C））を復号し、HD 2 1において、ライセンスL I Cが個別公開鍵K P o m 5により暗号化された暗号化ライセンスE（K P o m 5，L I C）が受理される（ステップS 2 4 2）。そして、復号処理部2 2 8は、暗号化ライセンスE（K P o m 5，L I C）をバスB S 3へ出力する。

コントローラ2 1 4の指示によって、暗号化ライセンスE（K P o m 5，L I C）は、復号処理部2 1 6において個別秘密鍵K o m 5によって復号され、HD 2 1においてライセンスL I Cが受理される（ステップS 2 4 3）。

コントローラ2 1 4は、ライセンスL I Cの受理を確認すると、ATAインターフェース部2 1 2および端子2 1 0を介してその旨を端末装置1 0に通知する。端末装置1 0のコントローラ1 0 8は、HDインターフェース部1 1 0およびバスB S 2を介して、HD 2 1においてライセンスL I Cが受理された旨の通知を受理すると、HD 2 1のセキュアデータ記憶部2 5 0において、その受信したライセンスL I Cを格納するL B A（格納L B A）をバスB S 2およびHDインタ

ーフェース 110 を介して HD 21 へ出力する（ステップ S 244）。HD 21
のコントローラ 214 は、端子 210 および ATA インターフェース部 212 を
介してライセンス LIC を格納する格納 LBA を受理すると（ステップ S 24
5）、その受理した格納 LBA をログメモリ 253 のバンク n に格納されるログ
5 の LBA 領域 2544 に記録する（ステップ S 246）。

そして、コントローラ 214 は、受理したライセンス LIC に含まれるライセ
ンス ID（LID）と、ステップ S 214 において受理したライセンス LID
（LID）とを比較し、一致しているか否かをチェックする（ステップ S 24
7）。コントローラ 214 は、LID が一致しており、受理したライセンス LI
10 C が正しいものであると判断すると、端末装置 10 から受理したセキュアデータ
記憶部 250 内の格納 LBA に対応する領域に、受理したライセンス LIC を記
憶する（ステップ S 248）。

コントローラ 214 は、指定された格納 LBA にライセンス LIC を記憶する
と、有効フラグ領域 252 のその格納 LBA に対応するフラグを“有効”にする
15 （ステップ S 249）。そして、コントローラ 214 は、さらに、ログメモリ 2
53 のバンク n に格納されたログのステータス ST1 を“受信済”にし（ステッ
プ S 250）、複製・移動セッションにおける一連の処理が終了したことを AT
A インターフェース部 212 および端子 210 を介して端末装置 10 に通知する。

そして、端末装置 10 において、HD 21 からの処理終了通知が受理されると、
20 HD 20 から HD 21 へのライセンス LIC の複製・移動セッションが正常終了
する。

一方、ステップ S 247 において、HD 20 のコントローラ 214 が、LID
が一致しておらず、受理したライセンス LIC が正しくないと判断すると、AT
A インターフェース部 212 および端子 210 を介してエラー通知を端末装置 1
25 0 へ出力し（ステップ S 251）、端末装置 10 においてエラー通知が受理され
ると（ステップ S 253）、HD 20 から HD 21 へのライセンス LIC の複製
・移動セッションが異常終了する。

ここで、配信セッションのときと同様に、図 18 および図 19 に示された複
製・移動セッションにおける一連の処理において、ステップ S 227 からステッ

ステップS 2 5 2の処理中に異常が発生し、処理が中断したときは、再書込処理の対象となる。

ここで、図1 8および図1 9に示された複製・移動セッションにおいて、ステップS 2 2 7からステップS 2 3 5までの処理を再書込処理の対象としたのは、この一連の処理がHD 2 0の内部処理であり、ステップS 2 2 6の終了後は、ステップS 2 3 8まで端末装置1 0においていずれのステップを処理中に処理が中断したかを特定できないため、すべてステップS 2 3 6が実行されてライセンスが無効化されたものとし、必ず再書込処理の対象としたものである。

そして、ステップS 2 3 6からステップS 2 4 7までの処理を再書込処理の対象としたのは、「移動」の場合、この間は、HD 2 0内のライセンスがステップS 2 3 6において無効化され、かつ、HD 2 1内に有効なライセンスが格納されていない状態であって、この間に処理が中断すると、対象となるライセンスが消失してしまうからである。

また、ステップS 2 4 8からステップS 2 5 0までの処理を再書込処理の対象としたのは、ステップS 2 4 9、S 2 5 0については、これらの処理はステップS 2 4 8におけるライセンス書込後の処理であるから本来は処理が終了しているところ、端末装置1 0からはステップS 2 4 8の終了が特定できないため、ステップS 2 4 8が終了していないものとみなして、ステップS 2 4 8からステップS 2 5 0を再書込処理の対象としたものである。なお、ステップS 2 4 8が終了して再書込処理が行なわれた場合には、再書込は拒否される。

また、ステップS 2 5 1の処理を再書込処理の対象としたのは、本来、この処理で処理が中断するのはかなり特殊な場合に限られるものであるが、端末装置1 0においては、ステップS 2 5 1において処理が中断したことを特定することができないため、再書込処理の対象としたものである。

なお、端末装置1 0において、上述したように当該セッションがライセンスの「複製」であると判断できる場合、あるいはステップS 2 2 7からステップS 2 3 5およびステップS 2 4 9からステップS 2 5 1のいずれかのステップで処理が中断したかを特定できる場合においては、必ずしも再書込処理とする必要はなく、図1 8および図1 9に示された複製・移動セッションを再度実行すればよい。

[移動／複製における再書込]

図 2 1～図 2 3 は、図 1 8 および図 1 9 において示した複製・移動セッションの処理フローにおけるステップ S 2 2 7 からステップ S 2 5 2 の処理中に異常が発生したときに行なわれる再書込処理の第 1 から第 3 のフローチャートである。

- 5 図 2 1 を参照して、端末装置 1 0 は、ステップ S 2 2 7 からステップ S 2 5 2 の処理中に異常が発生したと判断すると、ライセンス I D (L I D) とライセンス L I C の再送要求とをデータ列 L I D / / 再送要求として H D 2 0 へ出力する (ステップ S 3 0 1) 。 H D 2 0 では、コントローラ 2 1 4 が、端子 2 1 0 および A T A インターフェース部 2 1 2 を介して L I D / / 再送要求を受理する (ステップ S 3 0 1 a) 。そして、ログの複製処理を行なう (3 0 1 b) 。複製処理では、ログメモリ 2 5 3 内にステップ S 3 0 1 a において受理した L I D を含むログが格納されていないかを検索し、格納されていた場合、ログメモリ 2 5 3 の最も古いログを格納しているバンク n に、検索された L I D を含むログを複製し、変数 E R R = “偽” とする。一方、ログメモリ 2 5 3 内にステップ S 3 0 1 a において受理した L I D を含むログが格納されていない場合には、変数 E R R = “真” とする。この複製処理の詳細な動作は、図 1 6 に示すフローチャートに従って行なわれる。
- 10
- 15

- そして、コントローラ 2 1 4 は、ステップ S 3 0 1 a の処理結果の判定、すなわち、変数 E R R が “真” 、 “偽” のいずれであるかを判定する (ステップ S 3 0 1 b) 。 “真” の場合、受理した L I D を含むログがバンク n へ複製されたことを示すので、再送要求に対する処理を開始するために次のステップ S 3 0 2 へ移行する。 “偽” の場合、受理した L I D を含むログがログメモリ 2 5 3 に格納されていなかった、つまり、H D 2 0 において受理した L I D によって特定されるライセンス L I C の入出力処理がなされていなかったことを示すので、再送要求に対応不能と判断し、図 2 3 のステップ S 3 7 2 へ移行し、エラー通知を端末装置 1 0 に対して出力する。端末装置 1 0 においてはエラー通知が受理されると (ステップ S 3 7 3) 、処理が終了する。
- 20
- 25

H D 2 0 において、ステップ S 3 0 1 b において変数 E R R = “偽” を確認すると、コントローラ 2 1 4 は、ログメモリ 2 5 3 のバンク n に複製され、かつ、

格納されているログのステータス S T 1 の状態を確認する（ステップ S 3 0 2）。コントローラ 2 1 4 は、ステータス S T 1 が“送信待”または“送信済”でないとき、すなわち複製・移動セッションにおいてライセンス L I C の送信側でないときは、図 2 3 に示すステップ S 3 7 1 へ処理が移行する。

- 5 HD 2 0 のコントローラ 2 1 4 は、ステータス S T 1 が“送信待”または“送信済”であるときは、セッション鍵発生部 2 2 6 にセッション鍵を生成するように指示し、セッション鍵発生部 2 2 6 は、セッション鍵 K s 1 a を生成する（ステップ S 3 0 3）。セッション鍵 K s 1 b が生成されると、コントローラ 2 1 4 は、中断以前に受理した、ライセンス L I C の移動／複製先の HD 2 1 のクラス公開鍵 K P c m 1 を、ログメモリ 2 5 3 のバンク n に格納されたログから取得する（ステップ S 3 0 4）。ここで、移動／複製先の HD 2 1 から再びクラス証明書 I m c 1 を受理することなくログに記憶されるクラス公開鍵 K P c m 1 を用いるのは、再書込処理におけるなりすまし攻撃によるライセンス L I C の漏洩を防ぐためである。したがって、再び、クラス証明書 I m c 1 を受理する場合には、
- 10 HD 2 0 において、中断した処理において受理したクラス証明書と再書込処理において受理したクラス証明書とが同一か否かを確認する必要がある。たとえば、再書込処理において受理したクラス証明書 I m c 1 に含まれるクラス公開鍵とログに記録されるクラス公開鍵を比較して再書込処理を行なうか否かを判断する。

- 20 そして、HD 2 1 では、そのクラス公開鍵 K P c m 1 によって、セッション鍵 K s 1 b が暗号処理部 2 2 2 によって暗号化され、暗号化データ E (K P c m 1 , K s 1 b) が生成される（ステップ S 3 0 5）。コントローラ 2 1 4 は、生成された暗号化データ E (K P c m 1 , K s 1 b) とライセンス I D (L I D) とをデータ列 L I D / / E (K P c m 1 , K s 1 b) として ATA インターフェース部 2 1 2 および端子 2 1 0 を介して端末装置 1 0 へ出力する（ステップ S 3 0 6）。

25 端末装置 1 0 は、L I D / / E (K P c m 1 , K s 1 b) を受理すると（ステップ S 3 0 7）、受理した L I D / / E (K P c m 1 , K s 1 b) を HD 2 1 へ出力する（ステップ S 3 0 8）。

HD 2 1 において、コントローラ 2 1 4 は、端子 2 1 0 および ATA インター

フェース部 212 を介して L I D / / E (K P c m 1 , K s 1 b) を受理すると
(ステップ S 3 0 9)、バス B S 3 を介して E (K P c m 1 , K s 1 b) を復号
処理部 230 へ与える。そうすると、復号処理部 230 は、K c m 保持部 204
に保持される H D 21 に固有なクラス秘密鍵 K c m 1 によって復号処理を実行し
5 てセッション鍵 K s 1 b を復号し、セッション鍵 K s 1 b を受理する (ステップ
S 3 1 0)。

H D 21 のコントローラ 214 は、H D 20 で生成されたセッション鍵 K s 1
b の受理を確認すると、A T A インターフェース部 212 および端子 210 を介
してその旨を端末装置 10 に通知する。端末装置 10 のコントローラ 108 は、
10 H D インターフェース部 110 およびバス B S 2 を介して H D 21 からの通知を
受理すると、H D 21 のログメモリ 253 に格納されるログの H D 20 への出力
要求をバス B S 2 および H D インターフェース部 110 を介して H D 21 へ出力
する (ステップ S 3 1 1)。H D 21 のコントローラ 214 は、端子 210 およ
び A T A コントローラ 212 を介してログの出力要求通知を受理する (ステップ
15 S 3 1 2)。そして、H D 20 におけるステップ S 3 0 1 a と同様にログの複製
処理を行なう (ステップ S 2 1 3 a)。複製処理時、ログメモリ 253 内にステ
ップ S 3 0 9 において受理した L I D を含むログが格納されていないかを検索し、
格納されていた場合、ログメモリ 253 の最も古いログを格納しているバンク n
a に、検索された L I D を含むログを複製し、変数 E R R a = “偽” とする。一
20 方、ログメモリ 253 内にステップ S 3 0 9 において受理した L I D を含むログ
が格納されていない場合には、E R R a = “真” とする。このステップ S 3 1 2
a の詳細な動作は、図 16 に示すフローチャートに従って行なわれる。ただし、
H D 21 における処理と、H D 20 における同様の処理結果を区別するために変
数 n を変数 n a とし、変数 E R R を変数 E R R a とする。すなわち、図 16 のス
25 テップ S 1 1 2 b に相当する図 12 に示すフローチャートにおける変数 n を変数
n a に、変数 E R R を変数 E R R a にそれぞれ読替えればよい。

そして、コントローラ 214 は、ステップ S 3 1 2 a の処理結果の判定、すな
わち、E R R a が “真”、“偽” のいずれであるかを判定する (ステップ S 3 2
1 2 b)。“偽” の場合、受理した L I D を含むログがバンク n a へ複製された

ことを示すので、再送要求に対する処理を開始するために次のステップS 3 1 3
へ移行する。“真”の場合、受理したL I Dを含むログがログメモリ2 5 3に格
納されていなかった、つまり、HD 2 1において、ステップS 3 1 3において受
理したL I Dによって特定されるライセンスL I Cの入出力処理がなされなかつ
5 たことを示すので、再送要求に対応不能と判断し、図2 3のステップS 3 7 1へ
移行し、エラー通知を端末装置1 0に対して出力する。端末装置1 0においては、
エラー通知が受理されると（ステップS 3 7 3）、処理が終了する。

HD 2 1において、ステップS 3 1 2 bにおいてERR a = “偽”を確認する
と、コントローラ2 1 4は、ログメモリ2 5 3のバンクn aに格納されているロ
10 グの格納L B Aに対する領域に記憶されるライセンスL I CのライセンスI D
（L I D）と、ログメモリ2 5 3のバンクn aに格納されているログのライセン
スI D（L I D）とが一致するか否かを確認する（ステップS 3 1 3）。

コントローラ2 1 4は、ライセンスI D（L I D）が一致すると、さらに、ロ
グメモリ2 5 3のバンクn aに格納されているログの格納L B Aに対応する有効
15 フラグ領域2 5 2のフラグを確認し、そのライセンスL I Cが有効であるか無効
であるかを確認する（ステップS 3 1 4）。コントローラ2 1 4は、有効フラグ
領域2 5 2のフラグが“有効”であるときは、ログメモリ2 5 3のバンクn aに
格納されているログのステータスST 2を“データ有”に変更し（ステップS 3
1 5）、次の処理（ステップS 3 1 8）へ移行する。一方、コントローラ2 1 4
20 は、有効フラグ領域2 5 2のフラグが“無効”であるときは、ログメモリ2 5 3
のバンクn aに格納されているログのステータスST 2を“移動済”に変更し
（ステップS 3 1 6）、次の処理（ステップS 3 1 8）へ移行する。

また、コントローラ2 1 4は、ステップS 3 1 3において両ライセンスI D
（L I D）が一致しないときは、ログメモリ2 5 3のバンクn aに格納されてい
25 るログのステータスST 2を“データ無”に変更する（ステップS 3 1 7）。

ステータスST 2の変更処理がなされると、コントローラ2 1 4は、ログメモ
リ2 5 3のバンクn aからライセンスI D（L I D）、ステータスST 1、ST
2、セッション鍵K s 2 cおよび格納L B Aを取得する（ステップS 3 1 8）。
ここで、この処理は、図9および図10のフローチャートに従った配信セッショ

ンの中断に対する処理であるため、HD 2 1 のログメモリ 2 5 3 に格納されている当該処理のログに記憶されているセッション鍵はK s 2 aであるが、説明の関係上、ログメモリ 2 5 3 のバンク n から取得したセッション鍵をK s 2 cとしている。そして、コントローラ 2 1 4 は、取得したセッション鍵K s 2 cをバスBS 3 を介して暗号処理部 2 2 4 へ出力する。

暗号処理部 2 2 4 は、切換スイッチ 2 6 0 の接点 P b を介して復号処理部 2 3 0 より与えられるセッション鍵K s 1 bによってセッション鍵K s 2 cを暗号化し、E (K s 1 b, K s 2 c) 生成する (ステップS 3 1 9)。そして、暗号処理部 2 2 4 は、生成したE (K s 1 b, K s 2 c) をバスBS 3 に出力する。バスBS 3 に出力されたE (K s 1 b, K s 2 c) は、コントローラ 2 1 4 により受理され、コントローラ 2 1 4 は、ステップS 3 1 8において取得したデータとともに1つの受信ログL I D // E (K s 1 b, K s 2 c) // S T 1 // S T 2を生成し、そのハッシュ値H (L I D // E (K s 1 b, K s 2 c) // S T 1 // S T 2) を生成する (ステップS 3 2 0)。そして、コントローラ 2 1 4 は、ハッシュ値H (L I D // E (K s 1 b, K s 2 c) // S T 1 // S T 2) をバスBS 3 を介して暗号処理部 2 2 4 へ出力する。

暗号処理部 2 2 4 は、切換スイッチ 2 6 0 の接点 P b を介して復号処理部 2 3 0 より与えられるセッション鍵K s 1 bによって、バスBS 3 から取得したハッシュ値H (L I D // E (K s 1 b, K s 2 c) // S T 1 // S T 2) を暗号化し、署名データE (K s 1 b, H (L I D // E (K s 1 b, K s 2 c) // S T 1 // S T 2)) 生成する (ステップS 3 2 1)。そして、暗号処理部 2 2 4 は、生成したE (K s 1 b, H (L I D // E (K s 1 b, K s 2 c) // S T 1 // S T 2)) をバスBS 3 に出力する。

コントローラ 2 1 4 は、バスBS 3 から署名データを取得すると、ステップS 3 1 8において取得した受信ログを用いて、署名付き受信ログL I D // E (K s 1 b, K s 2 c) // S T 1 // S T 2 // E (K s 1 b, H (L I D // E (K s 1 b, K s 2 c) // S T 1 // S T 2)) を生成し、署名付き受信ログL I D // E (K s 1 b, K s 2 c) // S T 1 // S T 2 // E (K s 1 b, H (L I D // E (K s 1 b, K s 2 c) // S T 1 // S T 2)) と格納LB

Aとを、ATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS322）。

図22を参照して、端末装置10は、署名付き受信ログLID//E(Ks1b, Ks2c) //ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c) //ST1//ST2))と格納LBAとをHD21から受理すると（ステップS323）、受理したデータをHD20へ出力する（ステップS324）。

HD20において、コントローラ214は、署名付き受信ログLID//E(Ks1b, Ks2c) //ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c) //ST1//ST2))を受理すると（ステップS325）、受理した署名付き受信ログの検証を行なう（ステップS326）。検証処理は、以下のように行われる。

HD20のコントローラ214は、署名付き受信ログを受理すると、まず、受理した署名付き受信ログの後半部である署名データE(Ks1b, H(LID//E(Ks1b, Ks2c) //ST1//ST2))を復号処理部228へ出力するとともに、セッション鍵発生部226にセッション鍵Ks1bを発生するように指示する。そして、復号処理部228は、セッション鍵Ks1bによって署名データE(Ks1b, H(LID//E(Ks1b, Ks2c) //ST1//ST2))を復号し、HD21によって求められたハッシュ値を抽出する。

一方、HD20のコントローラ214は、署名付き受信ログの前半部である受信ログLID//E(Ks1b, Ks2c) //ST1//ST2のハッシュ値を演算し、復号処理部228により抽出されたハッシュ値と比較する。HD20のコントローラ214は、2つのハッシュ値が一致したと判断すると、HD21から受理した受信ログは、正当なデータを含むものとしてHD20において承認される。

ステップS326において承認されると、HD20のコントローラ214は、ステップS325において承認した受信ログに含まれるライセンスID(LID)をログメモリ253のバンクnに格納されるライセンスID(LID)と比較する（ステップS327）。

コントローラ 214 は、ライセンス ID (LID) が一致すると、受信ログに含まれる暗号データ E (Ks1b, Ks2c) を復号処理部 228 へ出力し、復号処理部 228 は、セッション鍵発生部 226 から受けるセッション鍵 Ks1b によってセッション鍵 Ks2c を復号し、セッション鍵 Ks2c が受理される
5 (ステップ S328)。そして、復号されたセッション鍵 Ks2c は、バス BS3 を介してコントローラ 214 へ出力される。続いて、コントローラ 214 は、エラー発生時のセッション鍵、すなわち、バンク n のログに記録されているセッション鍵 Ks2a と、今回、承認した受信ログに含まれていたセッション鍵 Ks2c とを比較する (ステップ S329)。コントローラ 214 は、セッション鍵
10 Ks2a とセッション鍵 Ks2c とが一致していると判断すると、受理したステータス ST1, ST2 の内容を確認する (ステップ S330)。

HD20 のコントローラ 214 は、受信した受信ログのステータス ST1 が“受信待”であり、受信ログのステータス ST2 が“データ無”であるとき、HD21 に送信したはずのライセンス LIC が何らかの異常により HD21 において受理されていないと判断する。そうすると、HD20 のコントローラ 214 は、
15 さらに、ログメモリ 253 のバンク n のログの格納 LBA に記憶されるライセンス LIC のライセンス ID (LID) と、ログメモリ 253 のバンク n のログのライセンス ID (LID) とが一致するか否かを確認する (ステップ S331)。HD20 のコントローラ 214 は、ライセンス ID (LID) が一致すると、さらに、ログメモリ 253 のバンク n のログの格納 LBA に対応する有効フラグ領域 252 のフラグを確認し、そのライセンス LIC が有効であるか無効であるかを確認する (ステップ S332)。そして、コントローラ 214 は、有効フラグ領域 252 のフラグが“無効”であるときは、その有効フラグ領域 252 のフラグを“有効”に変更する (ステップ S333)。一方、コントローラ 214 は、
20 有効フラグ領域 252 のフラグが“有効”であるときは、次の処理 (ステップ S334) へ移行する。そして、コントローラ 214 は、ログメモリ 253 のバンク n のログの格納 LBA と許可通知とを ATA インターフェース部 212 および端子 210 を介して端末装置 10 へ出力する (ステップ S334)。

端末装置 10 のコントローラ 108 は、HD20 から HD インターフェース部

1 1 0 およびバス B S 2 を介して対象のライセンス L I C が格納される格納 L B A と許可通知とを受理すると（ステップ S 3 3 5）、HD 2 1 に対してセッション鍵の生成の要求通知をバス B S 2 および HD インターフェース部 1 1 0 を介して HD 2 1 へ出力する（ステップ S 3 3 6）。

5 HD 2 1 は、端末装置 1 0 からセッション鍵の生成要求通知を受理すると、新たにセッション鍵 K s 2 b を生成し（ステップ S 3 3 7）、ログメモリ 2 5 3 のバンク n a のログに記憶されているセッション鍵 K s 2 c（K s 2 a）を、生成したセッション鍵 K s 2 b に、ログのステータス S T 1 を“受信待”に変更する（ステップ S 3 3 8）。

10 以下、ステップ S 3 3 9 からの一連の処理は、図 1 8 および図 1 9 において説明したステップ S 2 1 9 から処理終了までの一連の処理において、セッション鍵 K s 2 a に代えて新たに生成したセッション鍵 K s 2 b が使用される他は、同様の処理が行なわれる。したがって、ステップ S 3 3 9 に続く一連の処理の説明は繰返しになるので省略する。

15 なお、ステップ S 3 3 5 において処理を終了し、HD 2 0 にライセンスを残すことも可能である。この場合、図 1 8 および図 1 9 に示したフローチャートにしたがって、再度ライセンスを移動させることができる。

20 なお、図 2 1 ～図 2 3 のフローチャートに示されるライセンスの移動または複製における再書込処理の中断に対しては、ステップ S 3 0 1 ～S 3 4 4 およびステップ S 3 4 7 ～S 3 7 1 のいずれかのステップにおいて処理が中断した場合には、再び図 2 1 ～図 2 3 に示されるフローチャートに従って再書込処理を行なうことができる。一方、ステップ S 3 2 5 ～S 3 4 6 のいずれかのステップにおいて処理が中断した場合には、図 1 8 および図 1 9 のフローチャートに示されるライセンスの移動または複製の処理を最初から行なうことによって、処理を再開することができる。

25 このようにして、端末装置 1 0 に装着された複数のハードディスク間におけるライセンスの複製または移動に関しても、複製先または移動先の HD 2 1 から受取ったクラス証明書 C m 1 が有効であることを確認し、クラス証明書 C m 1 に含まれて送信されたクラス公開鍵 K P c m 1 によってライセンスの複製・移動が行

なわれる複数のハードディスク間でそれぞれ生成される暗号鍵（セッション鍵）をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、不正なハードディスクへのライセンスの複製または移動を禁止することができる。さらには、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、出力先のなりすましからライセンスを保護して、システムのセキュリティを向上させることができる。

さらに、ライセンスの複製・移動セッションの中断においても、配信セッションと同様に、受信側のデータ記憶装置であるHD 21における複製・移動セッションの対象となったライセンスLICに対する受信ログを送信側のデータ記憶装置であるHD 20へ送信し、HD 20において、自身のログメモリ 253に格納されるログの内容と、そのログに記憶される格納LBAによって特定されるセキュアデータ記憶部 250の領域に記憶されるライセンスLICとを比較し、さらに有効フラグ領域 252に記憶されるフラグを参照することによって、中断した複製・移動セッションがライセンスの移動を行なう処理である場合において、2つのデータ記憶装置HD 20およびHD 21に利用可能なライセンスが重複して存在することのない安全な再書込処理が提供される。

このように、本発明は、複製・移動セッションの中断によるライセンスLICの消失を回避し、迅速な処理を行なうことができるデータ記憶装置およびその処理手順を提供するとともに、再書込処理に至った場合でも安全に処理が行なわれ、確実な著作権保護を実現することができるデータ記憶装置およびその処理手順を提供する。

なお、図18～図23におけるHD 21の処理ステップS 202, 203, S 214, S 215, S 217～S 220, S 241～S 243, S 245～S 251, S 309, S 310, S 312～S 322, S 337～S 340, S 361～S 363, S 365～S 371は、図9、図10および図13～図15におけるHD 20の処理ステップS 2, S 3, S 16, S 17, S 19～S 22, S 33～S 35, S 37～S 43, S 109, S 110, S 112～S 122, S 136～S 139, S 150～S 152, S 154～S 160とそれぞれ同じである。すなわち、ライセンスの移動または複製時におけるHD 21の処理とライ

センスの配信処理時におけるHD 20の処理とは同じ処理であって、これらの処理は、いずれも、データ記憶装置（HD 20, HD 21）においてライセンスを書込むためのデータ記憶装置における処理である。

〔再生許諾〕

5 再び図5を参照して、コンテンツデータを再生する再生回路150を備えた端末装置10にデータ記憶装置としてのHD 20が装着され、コンテンツデータの再生許諾は、HD 20から端末装置10内の再生回路150に対して行なわれる。

図24は、端末装置10のユーザが端末装置10から暗号化コンテンツデータの再生リクエストを行なうことにより、端末装置10に装着されたHD 20から
10 端末装置10内の再生回路150へ再生許諾が行なわれる際の処理（再生許諾セッション）を説明するためのフローチャートである。

図24を参照して、端末装置10のユーザから所望のコンテンツデータの再生リクエストがなされると、端末装置10のコントローラ108は、バスBS2を介して再生回路150へクラス証明書の出力要求を出力する（ステップS40
15 1）。再生回路150において、認証データ保持部1502は、バスBS2からクラス証明書の出力要求を受けると（ステップS402）、保持しているクラス証明書Cp3=KPcp3//Icp3//E(Ka, H(KPcp3//Icp3))をバスBS2へ出力する（ステップS403）。

コントローラ108は、バスBS2からクラス証明書Cp3を受理すると（ス
20 テップS404）、受理したクラス証明書Cp3をバスBS2およびHDインターフェース部110を介してHD 20へ出力する（ステップS405）。

HD 20では、端末装置10からクラス証明書Cp3を受理すると（ステップS406）、受理したクラス証明書Cp3が正当なクラス証明書であるか否かを検証する（ステップS407）。検証処理は、複製・移動セッションにおけるス
25 テップS207において説明したのと同様の方法で行なわれ、説明は省略する。

ステップS407において、クラス証明書Cp3が正当な証明書であると判断された場合、コントローラ214は、クラス証明書Cp3を承認し、クラス証明書Cp3に含まれるクラス公開鍵KPcp3を受理する（ステップS408）。そして、次の処理（ステップS409）へ移行する。コントローラ214は、正

当なクラス証明書でない場合には、クラス証明書C p 3を非承認とし、クラス証明書C p 3を受理せずにエラー通知を端末装置10へ出力し（ステップS 4 3 5）、端末装置10においてエラー通知が受理されると（ステップS 4 3 6）、再生許諾セッションが終了する。

5 ステップS 4 0 8においてクラス公開鍵K P c p 3が受理されると、HD 2 0のセッション鍵発生部2 2 6は、セッション鍵K s 1 dを生成する（ステップS 4 0 9）。セッション鍵K s 1 dは、受理されたクラス公開鍵K P c p 3によって、暗号処理部2 2 2において暗号化され、暗号化データE（K P c p 3, K s 1 d）が生成される（ステップS 4 1 0）。

10 そして、コントローラ2 1 4は、暗号処理部2 2 2からバスB S 3を介して暗号化データE（K P c p 3, K s 1 d）を受けると、ATAインターフェース部2 1 2および端子2 1 0を介して端末装置10へ出力する（ステップS 4 1 1）。

15 端末装置10において、HDインターフェース部1 1 0およびバスB S 2を介してコントローラ1 0 8が暗号データE（K P c p 3, K s 1 d）を受理すると（ステップS 4 1 2）、コントローラ1 0 8は、受理した暗号化データE（K P c p 3, K s 1 d）をバスB S 2を介して再生回路1 5 0へ出力する（ステップS 4 1 3）。再生回路1 5 0の復号処理部1 5 0 6は、バスB S 2から暗号化データE（K P c p 3, K s 1 d）を受理すると（ステップS 4 1 4）、K c p保持部1 5 0 4に保持される再生回路1 5 0に固有なクラス秘密鍵K c p 3によって復号処理することによりセッション鍵K s 1 dを復号し、セッション鍵K s 1 dが受理される（ステップS 4 1 5）。

20 セッション鍵K s 1 dが受理されると、セッション鍵発生部1 5 0 8は、セッション鍵K s 2 dを生成し（ステップS 4 1 6）、生成したセッション鍵K s 2 dを暗号処理部1 5 1 0に与える。暗号処理部1 5 1 0は、復号処理部1 5 0 6から受けるセッション鍵K s 1 dをセッション鍵K s 2 dにより暗号化し、暗号化データE（K s 1 d, K s 2 d）を生成する（ステップS 4 1 7）。そして、暗号処理部1 5 1 0は、暗号化データE（K s 1 d, K s 2 d）をバスB S 2へ出力する（ステップS 4 1 8）。

25 コントローラ1 0 8は、バスB S 2から暗号化データE（K s 1 d, K s 2

d) を受理し (ステップ S 4 1 9)、受理したデータをバス B S 2 および H D インターフェース部 1 1 0 を介して H D 2 0 へ出力する (ステップ S 4 2 0)。

HD 2 0 のコントローラ 2 1 4 は、端子 2 1 0 および A T A インターフェース部 2 1 2 を介して暗号化データ E (K s 1 d, K s 2 d) を受理すると (ステップ S 4 2 1)、受理したデータをバス B S 3 へ出力する。復号処理部 2 2 8 は、セッション鍵発生部 2 2 6 から与えられたセッション鍵 K s 1 d を用いてバス B S 3 に出力された暗号化データ E (K s 1 d, K s 2 d) を復号し、H D 2 0 においてセッション鍵 K s 2 d が受理される (ステップ S 4 2 2)。そして、コントローラ 2 1 4 は、セッション鍵 K s 2 d が受理されると、その旨の通知を A T A インターフェース部 2 1 2 および端子 2 1 0 を介して端末装置 1 0 へ出力する。

端末装置 1 0 のコントローラ 1 0 8 は、H D インターフェース部 1 1 0 およびバス B S 2 を介して H D 2 0 においてセッション鍵 K s 2 d が受理された旨の通知を受理すると、再生リクエストのあったコンテンツデータに対応する対象のライセンス L I C が格納されているセキュアデータ記憶部 2 5 0 の L B A をバス B S 2 および H D インターフェース部 1 1 0 を介して H D 2 0 へ出力する。

H D 2 0 のコントローラ 2 1 4 は、端子 2 1 0 および A T A インターフェース部 2 1 2 を介して対象のライセンス L I C が格納されている L B A を受理すると (ステップ S 4 2 4)、その L B A に格納されるライセンス L I C に対応する有効フラグ領域 2 5 2 のフラグが “有効” であるか “無効” であるかを確認する (ステップ S 4 2 5)。

コントローラ 2 1 4 は、有効フラグ領域 2 5 2 のフラグが “有効” であると、受理した L B A に基づいて、対象のライセンス L I C をセキュアデータ記憶部 2 5 0 から取得する (ステップ S 4 2 6)。そして、コントローラ 2 1 4 は、取得したライセンス L I C に含まれる制御情報 A C の内容を確認する (ステップ S 4 2 7)。コントローラ 2 1 4 は、制御情報 A C において利用回数が指定されているときは、制御情報 A C の利用回数を 1 増分し、次の処理 (ステップ S 4 2 9) へ移行する。一方、コントローラ 2 1 4 は、制御情報 A C により再生制限がかけられていないときは、取得したライセンス L I C に含まれるコンテンツ鍵 K c をバス B S 3 へ出力する。

暗号処理部 224 は、復号処理部 228 から受けるセッション鍵 K_{s2d} によりバス $BS3$ 上に出力されたコンテンツ鍵 K_c を暗号化して暗号化データ $E(K_{s2d}, K_c)$ を生成し (ステップ $S429$)、生成したデータをバス $BS3$ へ出力する。そして、コントローラ 214 は、バス $BS3$ 上に出力された暗号化データ $E(K_{s2d}, K_c)$ を ATA インターフェース部 212 および端子 210 を介して端末装置 10 へ出力する (ステップ $S430$)。

端末装置 10 のコントローラ 108 は、 HD インターフェース部 110 およびバス $BS2$ を介して暗号化データ $E(K_{s2d}, K_c)$ を受取りすると (ステップ $S431$)、受取ったデータをバス $BS2$ へ出力する (ステップ $S432$)。

再生回路 150 の復号処理部 1512 は、バス $BS2$ から暗号化データ $E(K_{s2d}, K_c)$ を受取りすると (ステップ $S433$)、セッション鍵発生部 1508 から与えられるセッション鍵 K_{s2d} を用いて暗号化データ $E(K_{s2d}, K_c)$ を復号する。これにより、再生回路 150 においてコンテンツ鍵 K_c が受取られ (ステップ $S434$)、一連の再生許諾セッションの処理が正常終了する。

一方、ステップ $S425$ において、有効フラグ領域 252 のフラグが “無効” であったとき、またはステップ $S427$ において、制御情報 AC に含まれる内容が再生不可であったときは、コントローラ 214 は、端末装置 10 に対してエラー通知を出力し (ステップ $S435$)、端末装置 10 においてエラー通知が受取られると (ステップ $S436$)、再生許諾セッションが終了する。

このようにして、データ記憶装置である $HD20$ から端末装置 10 に備えられる再生回路 150 への再生許諾に関しても、再生回路 150 が正規のクラス証明書 $Cp3$ を保持していること、およびクラス証明書 $Cp3$ に含まれて送信されたクラス公開鍵 K_{Pcp3} が有効であることを確認した上でコンテンツ鍵 K_c が再生回路 150 へ送信され、不正なコンテンツデータの再生を禁止することができる。

なお、フローチャートにおいて図示しないが、再生回路 150 は、コンテンツの再生許諾がなされ、コンテンツ鍵 K_c を受取りすると、 $HD20$ から出力された暗号化コンテンツデータ $E(K_c, D_c)$ を復号処理部 1514 において復号し、再生部 1516 において復号処理部により復号されたデータ D_c が再生され、 D

A変換部1518によりデジタル／アナログ変換されてモニタやスピーカなどが接続される端子1520へ再生信号が出力される。

このように、HD20では、ライセンスの漏洩が無いように安全に保護し、記憶、入出力の管理を行なうために、

- 5 (1) 他の装置（ライセンス提供装置または他のHD）からライセンスの提供を受けて格納する書込処理（図9および図10におけるHD20および図21～図23におけるHD21の処理）
- (2) 書込処理の中断から、書込処理を再開する再書込処理（図13～図15におけるHDおよび図21～図23におけるHD21の処理）
- 10 (3) 他のHDに対してライセンスを移動または複製する提供処理（図16～図18におけるHD20の処理）
- (4) 提供処理の中断から、移動複製処理を再開する再提供処理（ライセンスの提供元としての再書込処理、図21～図23におけるHD20の処理）
- (5) 暗号化コンテンツデータを復号することを目的として再生回路に対してコ
15 ンテンツ鍵Kcを提供する再生許諾処理（図24におけるHD20の処理）

の5つの処理を、暗号技術によって実現している。

なお、上述した全ての説明においては、コンテンツデータに対するライセンスについて説明したが、対象は、上述したライセンスに限られるものではなく、秘密にする必要がある機密データ一般に拡大されうる。上述した手段によって、デ
20 ータの機密性が保護され、かつ、データ記憶装置における機密データの特定に関する本発明の目的が達成できるからである。

〔実施の形態2〕

実施の形態1においては、HD20は、図13～図15のフローチャートに示される再書込処理および図21～図23のフローチャートに示される再提供処理
25 において、再書込／提供処理を開始するにあたって、処理の可否を判断するために、再書込／提供処理の対象となるライセンスに対する直前のログを検索する。そして、対応したログが検索された場合、検索したログをログメモリ253のバンクnに複製して、以後の処理においてはバンクnに格納されたログを処理の手順に従って更新していくものとして説明した。

しかし、再書込処理においては、複製したログはライセンスの提供側に対して直前の処理に対するログとして出力した後、図 1 4 のステップ S 1 3 7 において、その内容が書換えられてしまう。ログの複製は、古いログが格納されたバンクから順に新たなログの格納バンクに向けて循環的に使用していくログメモリ 2 5 3 の特性に由来するものであり、再書込処理の初期における中断（図 1 4 のステップ S 1 3 6 以前）においても、再書込処理に対応するログが、より長くログメモリ 2 5 3 に保持されることを目的としている。

したがって、十分に大きなログメモリ 2 5 3 を備えた HD においては、再書込処理における検索されたログの複製を行なうことなく、検索されたログが格納されていたバンクから直接出力するように構成することも可能である。この場合、ステータス S T 2 の変更（ステップ S 1 1 5, S 1 1 6, S 1 1 7）は、当該バンクのログに対して行なわれ、出力するためのログの取得（ステップ S 1 1 8）は、当該バンクから行なわれることとなる。

また、ログの複写がなされないため、再書込処理に対応するログを格納するためのバンクは、図 1 4 のステップ S 1 3 7 において確保される。したがって、ステップ S 1 3 7 は、「ログメモリの最も古いログを格納しているバンク n a に新たなログを格納」と変更される。

さらに、HD 2 1 も同様に処理を変更することが可能である。その他の全ての処理は、実施の形態 1 と同じである。なお、この処理の変更によってライセンスの安全性は何ら変化することはなく、実施の形態 1 と同様の効果を得ることができる。

〔実施の形態 3〕

ライセンスの再書込処理と同様に、ライセンスの再提供処理において、検索されたログの複製を行なうことなく、検索されたログが格納されていたバンクから直接読出し、再提供の可否を判定することも可能である。図 2 1 のステップ S 3 0 1 a において複製を行なうことなく、図 2 1 のステップ S 3 0 2 および図 2 2 のステップ S 3 2 9, S 3 3 1, S 3 3 2 において検索されたログが格納されていたバンクから直接ログを取得するように処理を変更すればよい。その他の全ての処理は、実施の形態 1 と同じである。

この処理の変更によってライセンスの安全性は、何ら変化することはなく、実施の形態 1 と同様の効果を得ることができる。また、実施の形態 2 と組み合わせることも可能である。

〔実施の形態 4〕

5 HD 20 の実装における処理を軽減するためには、通常の手入処理および再手入処理は、より共通していることが望ましい。そこで、実施の形態 1 における「セッション鍵要求」移行の HD 20 における処理、すなわち、通常の手入処理（図 9 のステップ S 19 ～ S 22、図 10 のステップ S 33 ～ S 35、S 38 ～ S 43）と再手入処理（図 14 のステップ S 136 ～ S 139、図 15 のステップ S 150 ～ S 152、S 154 ～ S 160）を共通とする。この場合、図 9 の
10 ステップ S 20 と図 14 のステップ S 137 とを同一処理とすることで容易に実現できる。

この場合、ステップ S 137 をステップ S 20 と同一処理とし、“ログメモリの最も古いログを格納しているバンク n b に新たなログを格納”とする。また、
15 詳細な処理は、図 11 および図 12 のフローチャートに従い、変数 n を変数 n b と読替えればよい。また、変数 n を変数 n b と読替えるのは、図 13 および図 14 のステップ S 137 までの処理における変数 n と区別するためである。これに伴って、図 14 および図 15 のステップ S 137 以降のステップ S 154、S 155、S 159 におけるバンク n を全てバンク n b と読替える。

20 同様に、移動複製セッションでは、図 21 ～図 23 のフローチャートに示されるステップ S 342 以降の処理と、図 16 ～図 18 のフローチャートに示されるステップ S 222 以降の処理との違いが、ログの記録の違い（図 23 のステップ S 345 と図 18 のステップ S 225 との違い）のみである。図 23 のステップ S 345 の処理を図 18 のステップ S 225 と同一の処理とすることによって HD 20 の実装を容易にすることができる。この場合、ステップ S 345 をステップ S 20 と同一処理とし、“ログメモリの最も古いログを格納しているバンク n b に新たなログを格納”とする。また、詳細な処理は、図 20 および図 12 のフローチャートに従い、変数 n を変数 n b と読替えればよい。また、変数 n を変数 n b と読替えるのは、図 21 および図 22 のステップ S 245 までの処理におけ
25

る変数 n と区別するためである。これに伴って、図 2 3 のステップ S 3 4 5 以降のステップ S 3 4 8, S 5 7 におけるバンク n を全てバンク $n b$ と読替える。

その他の全ての処理は、実施の形態 1 と同一である。また、処理の変更によってライセンスの安全性は何ら変化することなく、実施の形態 1 と同様な効果を得ることができる。さらに、HD 2 1 も同様に処理を変更することが可能である。

このように、通常書込処理および再書込処理の共通化によって、実施の形態 1 と同様なライセンスの安全な管理を実現した上で実装する処理量の軽減を図ることができる。

[実施の形態 5]

ログの記録開始タイミングを明確にするために、全ての処理において HD 外部からライセンス ID (LID) を受理することによって、ログメモリ 2 5 3 からバンクを 1 つ確保し、当該処理に対するログを記録するように変更した実施の形態 5 について説明する。

まず、実施の形態 5 におけるライセンスの配信動作について説明する。

実施の形態 5 においては、ライセンス提供措置 4 0 から HD 2 0 へのライセンスの配信は、図 2 5 および図 2 6 に示すフローチャートに従って行なわれる。図 2 5 および図 2 6 に示すフローチャートは、図 9 および図 1 0 に示すフローチャートのステップ S 1 6 とステップ S 1 7 との間にステップ S 1 6 a を挿入し、ステップ S 2 0 をステップ S 2 0 1 a に代えたものであり、その他は図 9 および図 1 0 に示すフローチャートと同じである。

ステップ S 1 6 a の詳細な動作は、図 2 7 に示すフローチャートに従って行なわれる。図 2 7 を参照して、HD 2 0 にコントローラ 2 1 4 は、ステップ S 1 6 の後、最新のログが格納されているバンク $n-1$ を特定し、バンク n に格納されている管理番号 m を取得する (ステップ S 1 6 b)。そして、このステップ S 1 6 b の詳細な動作は、図 1 2 に示すフローチャートに従って行なわれる。

コントローラ 2 1 4 は、ステップ S 1 6 b の後、管理番号 $m+1$ 、およびステップ S 1 6 で受理したライセンス ID (LID) をバンク n に格納し、バンク n に格納されたログの ST 1 領域 2 5 4 4 を“受信待”に設定する (ステップ S 1 6 c)。これにより、図 2 5 に示すステップ S 1 6 a の動作が終了する。

また、コントローラ 214 は、ステップ S 19 の後、ログメモリ 253 のバンク n に格納されたログの K s 2 x 領域 2543 に、ステップ S 19 で受理したセッション鍵 K s 2 a を記録する（ステップ S 201 a）。

その他は、実施の形態 1 において説明したとおりである。

5 [配信における再書込]

実施の形態 5 におけるライセンスの配信が途中で中断した場合のライセンスの再書込の動作は、図 13～図 15 に示すフローチャートに従って行なわれる。その詳細な動作は実施の形態 1 において説明したとおりである。

 [移動／複製]

10 図 28 および図 29 は、図 17 に示すライセンスの複製・移動が可能なシステムにおいて、端末装置 10 のユーザが端末装置 10 から暗号化コンテンツデータのライセンスの複製または移動のリクエストを行なうことにより、端末装置 10 を介して端末装置 10 に装着された HD 20 から HD 21 へライセンスの複製または移動が行なわれる際の処理（複製・移動セッション）を説明するための実施
15 の形態 5 における第 1 および第 2 のフローチャートである。

 図 28 および図 29 に示すフローチャートは、図 18 および図 19 に示すフローチャートのステップ S 207 とステップ S 209 との間にステップ S 208 を挿入し、ステップ S 214 とステップ S 215 との間にステップ S 214 a を挿入し、ステップ S 218 をステップ S 218 a に代え、ステップ S 225 をステ
20 ップ S 225 a に代えたものであり、その他は図 18 および図 19 に示すフローチャートと同じである。

 図 28 を参照して、HD 20 のコントローラ 214 は、ステップ S 207 において HD 21 からの証明書 C m 1 を承認したとき、ログメモリ 253 のうち最も古いログが格納されたバンク n に新たなログを格納する（ステップ S 208）。
25 このステップ S 208 の詳細な動作は、図 30 に示すフローチャートに従って行なわれる。

 図 30 を参照して、ステップ S 208 は、HD 20 においてログメモリ 253 の最新ログが記録されたバンク n-1 を特定し、かつ、バンク n-1 に格納された管理番号 m を取得するステップ S 208 a と、バンク n に、管理番号 m+1、

ライセンスID (LID)、およびクラス公開鍵K P c m yを格納し、かつ、S
T 1領域2544のステータスST 1を“送信待”に設定するステップS 208
bとから成る。そして、ステップS 208 aの詳細な動作は、図12に示すフロ
ーチャートに従って行なわれる。したがって、コントローラ214は、図12お
よび図30に示すフローチャートに従って、ステップS 206において受理した
5 ライセンスID (LID)とHD 21のクラス公開鍵K P c m 1と、“送信待”
に設定されたステータスST 1とを記録した新たなログをバンク nに格納する。

また、HD 21のコントローラ214は、ステップS 214の後、最も古いロ
グが格納されたバンク n aに新たなログを格納する(ステップS 214 a)。こ
10 のステップS 214 aの詳細な動作は、上述した図12および図27に示すフロ
ーチャートに従って行なわれる。ただし、変数nは、変数n aに読替える。

したがって、HD 21のコントローラ214は、図12および図27に示すフ
ローチャートに従って、ステップS 214において受理したライセンスID (L
ID)と、“受信待”に設定されたステータスST 1とを記録した新たなログを、
15 ログメモリ254の中で最も古いログが格納されていたバンク n aに格納する
(ステップS 214 a)。

さらに、HD 21のコントローラ214は、ステップS 217の後、ログメモ
リ253のバンク n aにステップS 217において生成されたセッション鍵K s
2 aを格納する(ステップS 218 a)。

さらに、HD 20のコントローラ214は、ステップS 224の後、ログメモ
リ253のバンク nに、ステップS 224で受理したセッション鍵K s 2 aを格
20 納する(ステップS 225 a)。

その他は、実施の形態1において説明したとおりである。

[移動／複製における再書込]

25 実施の形態5におけるHD 21からHD 20へのライセンスの移動・複製セッ
ションが途中で中断した場合のライセンスの再書込動作は、図21～図23に示
すフローチャートに従って行なわれる。したがって、その詳細な動作は実施の形
態1で説明したとおりである。

このように、実施の形態5では、実施の形態1と同様に安全なライセンスの再

書込／提供処理を実現し、かつ、それぞれの処理におけるログの発生タイミングを明確にするとともに、実施の形態 3 と同様に、通常書込／再書込処理の共通化によって実装する処理量の軽減を図ることができる。なお、HD 2 1 も同様に処理を変更することが可能である。

- 5 今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

10 産業上の利用可能性

この発明は、機密データの入出力処理に関する履歴情報を重複することなく複数格納できるデータ記憶装置に適用可能である。

請求の範囲

1. 一定の手順に従って機密データの入出力を行ない、前記機密データを記憶し、かつ、前記一定の手順の進行に従って履歴情報を格納あるいは当該履歴情報を随時更新するデータ記憶装置（20）であって、

外部とデータの入出力を行なうインターフェース（212）と、

複数の前記機密データを格納するデータ記憶部（270）と、

前記機密データの入出力に関する複数の履歴情報を格納するログ記憶部（253）と、

前記機密データの入出力を制御する制御部（214）とを備え、

前記ログ記憶部（253）は、それぞれ1つの前記履歴情報を格納する2つ以上の領域を循環的に利用するリングバッファとして設けられており、

前記ログ記憶部（253）に記憶される複数の履歴情報の各々は、当該履歴情報を記憶した入出力対象の機密データを識別する識別情報を含み、

前記制御部（214）は、前記機密データの入出力の処理が開始されたことに伴い入出力の対象となった機密データを識別する識別情報を前記インターフェース（212）を介して受取り、前記ログ記憶部（253）の複数の領域（2531～253N）を所定の順序で検索して、前記ログ記憶部（253）に格納されている最も古い履歴情報を格納する領域を最古領域として特定し、その特定した最古領域に前記受取った識別情報を含む前記機密データの入出力処理に対する履歴情報を新たに格納する、データ記憶装置。

2. 履歴情報の出力要求に対して履歴情報の一部または全てを出力する履歴情報の出力処理において、

前記制御部（214）は、入出力の対象となる機密データの識別情報を前記インターフェース（212）を介して受取り、前記ログ記憶部（253）の複数の領域（2531～253N）を所定の順序で検索して、前記最古領域と、前記受取った識別情報を含む最も新しい履歴情報を格納する領域を最新領域として特定し、前記最新領域に格納されている履歴情報の一部または全てを前記インターフェース（212）を介して出力する、請求の範囲第1項に記載のデータ記憶装置。

3. 履歴情報の出力を伴う前記機密データの入力処理において、

前記制御部（214）は、入出力の対象となる機密データの識別情報を前記インタフェース（212）を介して受取り、前記ログ記憶部（253）の複数の領域（2531～253N）を所定の順序で検索して、前記最古領域と、前記受取った識別情報を含む最も新しい履歴情報を格納する最新領域とを特定し、その特定した最新領域に格納されている履歴情報の一部または全てを、特定した最古領域に複製することによって前記機密データの入力処理に対する新たな履歴情報として格納し、前記特定された最古領域に格納された履歴情報の一部または全てを前記インタフェース（212）を介して出力する、請求の範囲第1項に記載のデータ記憶装置。

4. 他の装置によって前記一定の手順の進行によって記録されたもう1つの履歴情報の入力に伴う前記機密データの再出力処理において、

前記制御部（214）は、入出力の対象となる機密データの識別情報および前記もう1つの履歴情報とを前記インタフェース（212）を介して受取り、前記最古領域および前記最新領域を特定し、その特定した最新領域に格納された履歴情報と、前記受取ったもう1つの履歴情報とに基づいて、前記機密データを出力するか否かを判定する、請求の範囲第2項または請求の範囲第3項に記載のデータ記憶装置。

5. 他の装置によって前記一定の手順の進行に従って記録されたもう1つの履歴情報の入力に伴う前記機密データの出力処理において、

前記制御部（214）は、入出力の対象となる機密データの識別情報および前記もう1つの履歴情報を前記インタフェース（212）を介して受取り、前記最古領域および前記最新領域を特定し、その特定した最新領域に格納されている履歴情報の一部または全てを、特定した最古領域に複製することによって前記機密データの出力処理に対する新たな履歴情報として格納し、前記特定した最古領域に格納された履歴情報と、前記受取ったもう1つの履歴情報とに基づいて、前記機密データを出力するか否かを判定する、請求の範囲第2項または請求の範囲第3項に記載のデータ記憶装置。

6. 前記最古領域を特定した後、

前記制御部（２１４）は、前記入出力処理における一定の手順が終了あるいは中止されるまでの間、前記特定された最古領域に格納された履歴情報を、当該手順の進行に従って随時更新する、請求の範囲第１項に記載のデータ記憶装置。

- 5 7. 前記複数の履歴情報の各々は、前記ログ記憶部（２５３）へ記憶された順序を識別するための管理番号（２５４１）をさらに含み、

前記管理番号（２５４１）は、前記ログ記憶部（２５３）に連続して配置された２つの領域に格納された２つの履歴情報に含まれる各々の管理番号に基づいて、古い履歴情報が格納される前記最古領域を検出する、請求の範囲第１項に記載のデータ記憶装置。

- 10 8. 前記ログ記憶部（２５３）は、 N （ N は２以上の自然数）個の領域（２５３１～２５３ N ）を循環的に利用するリングバッファからなり、

前記管理番号（２５４１）は、 M （ M は、 $N < M$ を満たす自然数）の剰余系からなる、請求の範囲第７項に記載のデータ記憶装置。

- 15 9. 前記制御部（２１４）は、前記ログ記憶部（２５３）に連続して配置された２つの領域に格納された２つの履歴情報に含まれる各々の管理番号（２５４１）を取得し、その取得した２つの管理番号（２５４１）の差に基づいて、２つの当該管理番号（２５４１）を含む２つの履歴情報が連続して格納されたか否かを判定し、２つの履歴情報が不連続に格納された履歴情報であるとき、前記連続する２つの領域のうち、後続領域を前記最古領域として検出する、請求の範囲第８項
20 に記載のデータ記憶装置。

FIG. 1

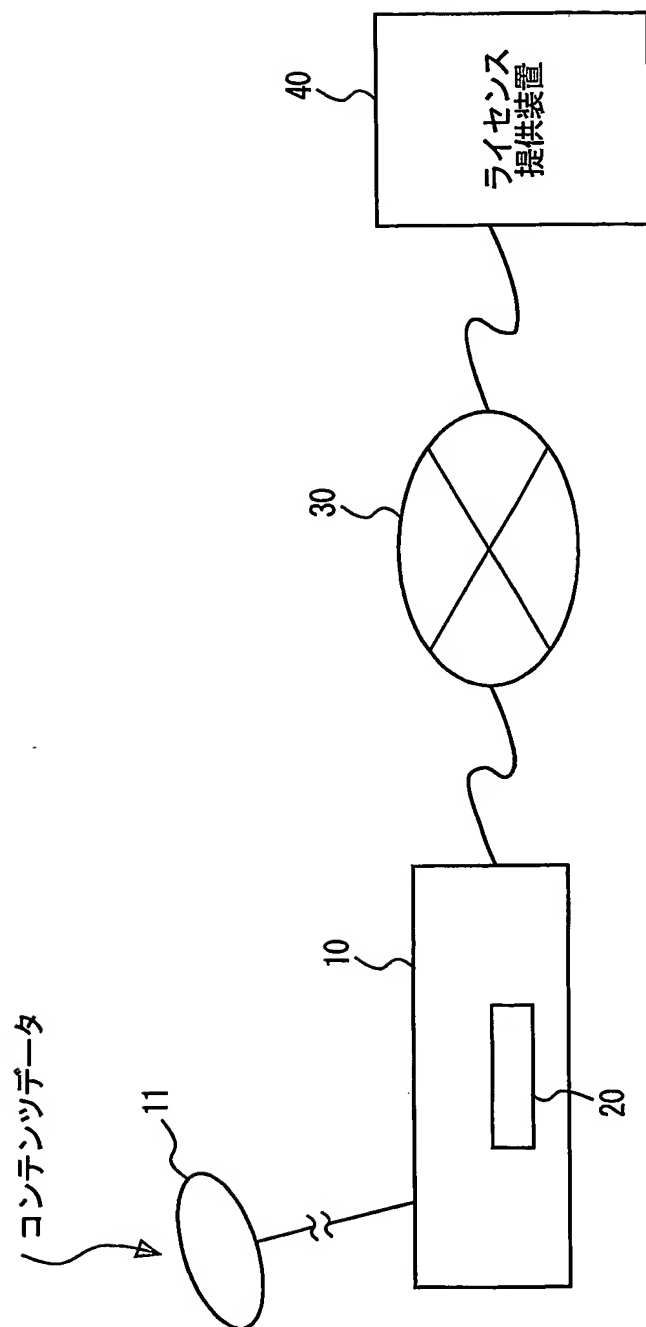


FIG. 2

記号	名称	属性	特性
Dc	データ	データ固有	例：音楽データ、朗読データ、教材データ、画像データ Kcにて暗号化した暗号化コンテンツデータ E(Kc, Dc)として記録管理される
Di	データ情報	データ固有	Dcに付随する平文データ。DIDを含む
DID	データID	データ固有	DcおよびKcを特定するための管理コード
Kc	コンテンツ鍵	データ固有	暗号データを暗号／復号する共通鍵
AC	制御情報	ライセンス固有	再生やライセンスの取扱いに関する制限事項
LID	ライセンスID	ライセンス固有	ライセンスを特定するための管理コード
LIC	ライセンス	ライセンス固有	Kc//AC//DID//LIDの総称

FIG. 3

記号	名称	特性
ライセンス提供装置	認証鍵	認証局にて証明書を検証する公開復号鍵 ライセン্স提供側にて運用される
	セッション鍵	ライセン্সの配信ごとに生成される一時鍵 共通鍵
	マスタ鍵	クラス証明書作成のために使用する秘密暗号鍵 認証局にて運用される
	認証鍵	認証局にて証明書を検証する公開復号鍵 ライセン্স提供側にて運用される
データ記録装置 (ハードディスク)	クラス公開鍵	機器のクラス(種類などの一定の単位ごと)に付与される暗号鍵 「J」はクラスを識別するための識別子
	クラス秘密鍵	クラス公開鍵「Pcmj」にて暗号化されたデータを復号する非対称な復号鍵
	クラス情報	クラスごとの機器およびクラス公開鍵に関する情報データ
	クラス証明書	$Qmj = K(Pcmj // lcmj // E(Ka, H(KPcmj // lcmj)))$ 認証鍵「Pal」によってその正当性が確認できる
	個別公開鍵	データ記録装置ごとに固有な値を持つ個別公開暗号鍵 「Z」はデータ記録装置を識別するための識別子
	個別秘密鍵	個別公開鍵「Pomz」にて暗号化されたデータを復号する非対称な復号鍵
	セッション鍵	ライセン্সの授受ごとにライセン্স提供側で生成される一時鍵 共通鍵
	セッション鍵	ライセン্সの授受ごとにライセン্স受理側で生成される一時鍵 共通鍵
	クラス公開鍵	機器のクラス(種類などの一定の単位ごと)に付与される暗号鍵 「J」はクラスを識別するための識別子
	クラス秘密鍵	クラス公開鍵「Pcpj」にて暗号化されたデータを復号する非対称な復号鍵
再生回路	クラス情報	クラスごとの機器およびクラス公開鍵に関する情報データ
	クラス証明書	$Qpy = K(Pcpj // lcpj // E(Ka, H(KPcpj // lcpj)))$ 認証鍵「Pal」によってその正当性が確認できる
	セッション鍵	ライセン্সの授受ごとにライセン্স受理側で生成される一時鍵 共通鍵

FIG. 4

40

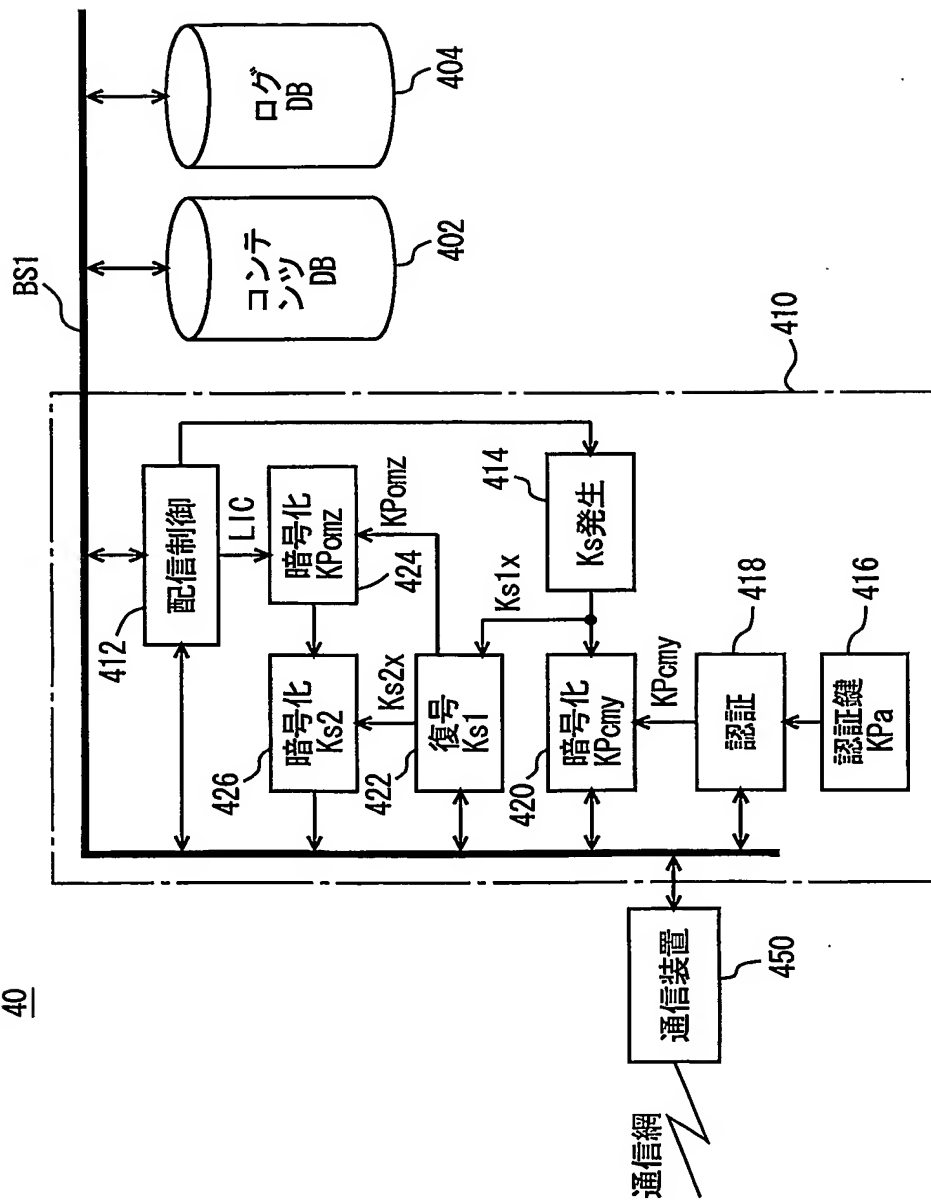


FIG. 5

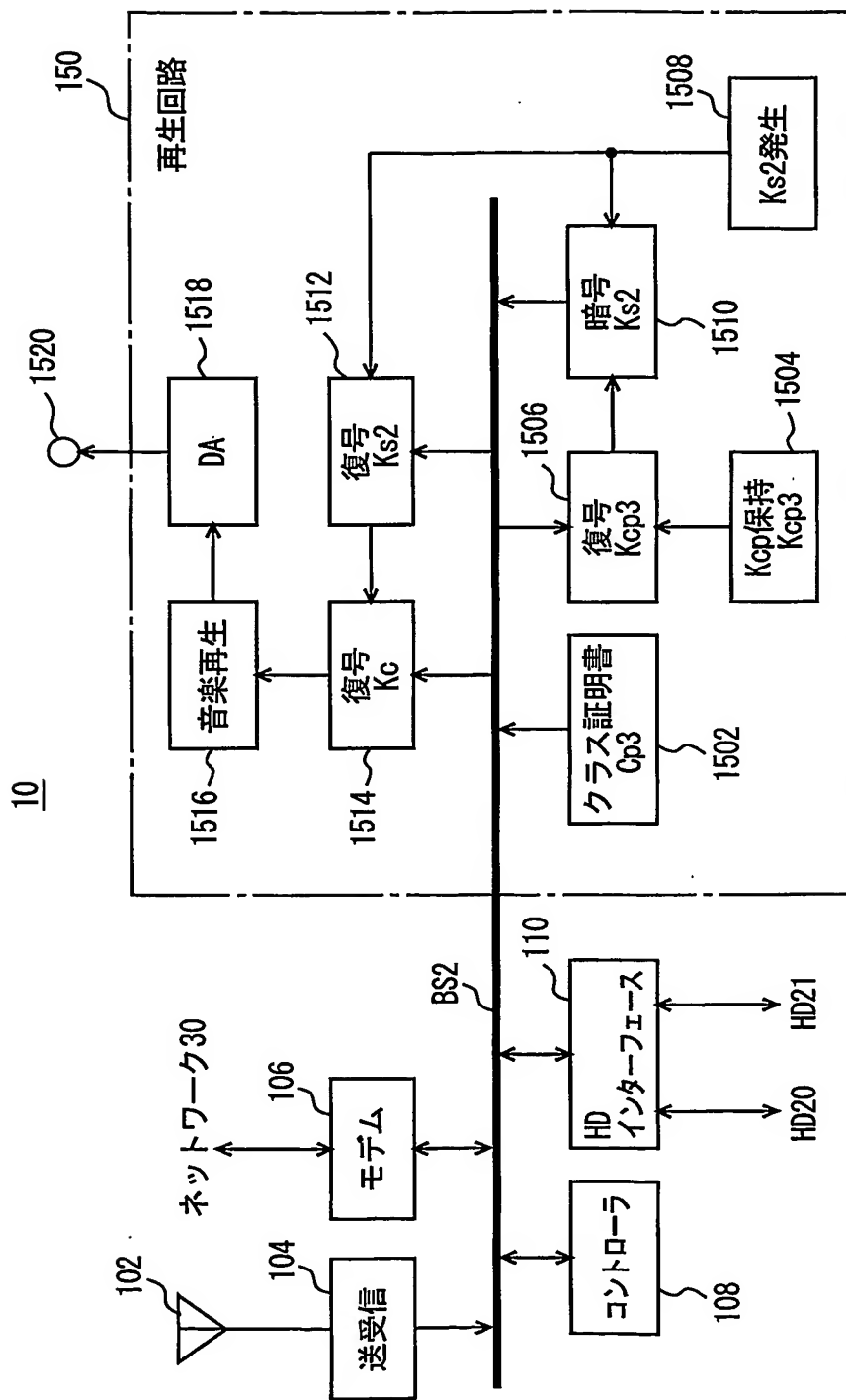


FIG. 6

20, 21

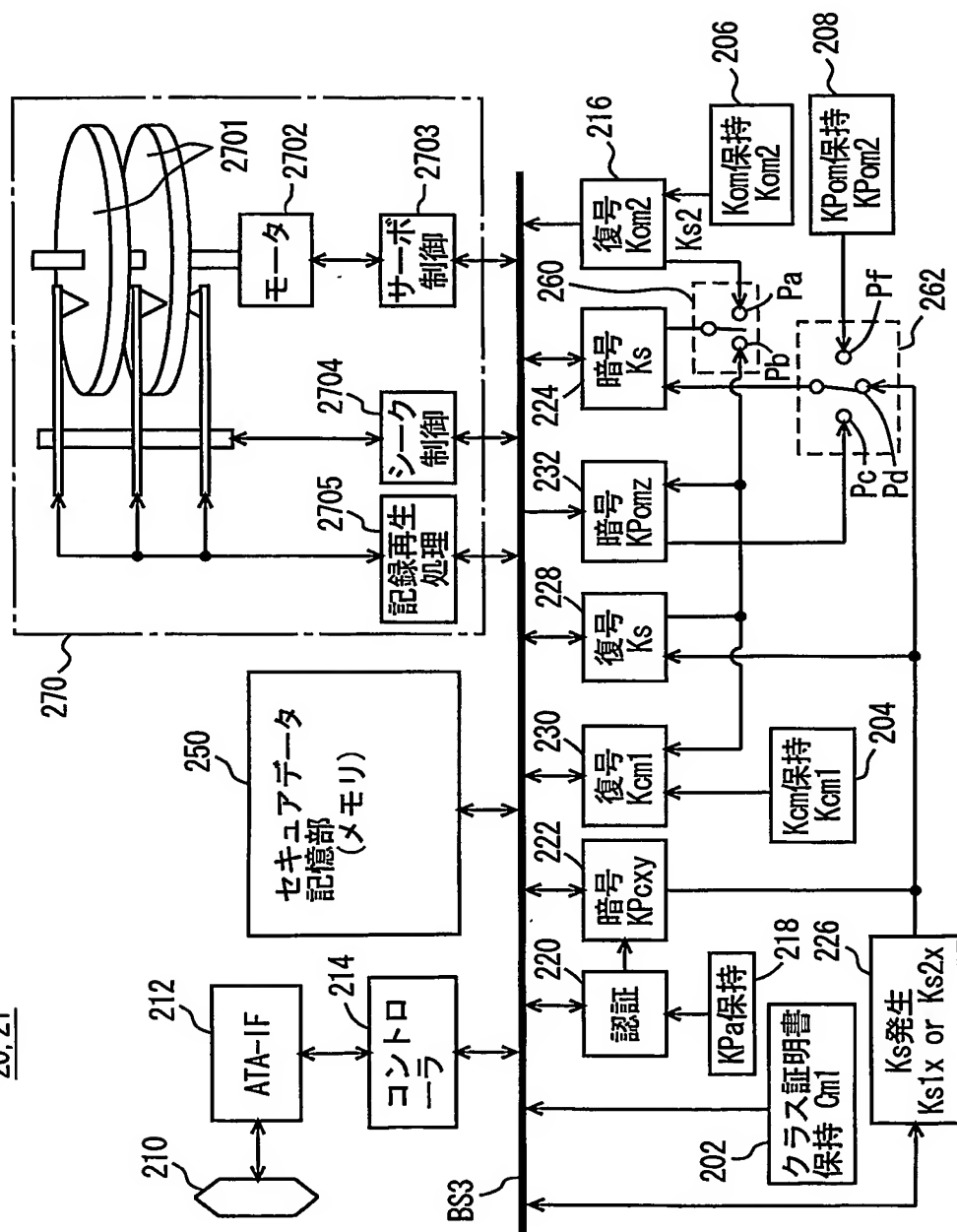


FIG. 7

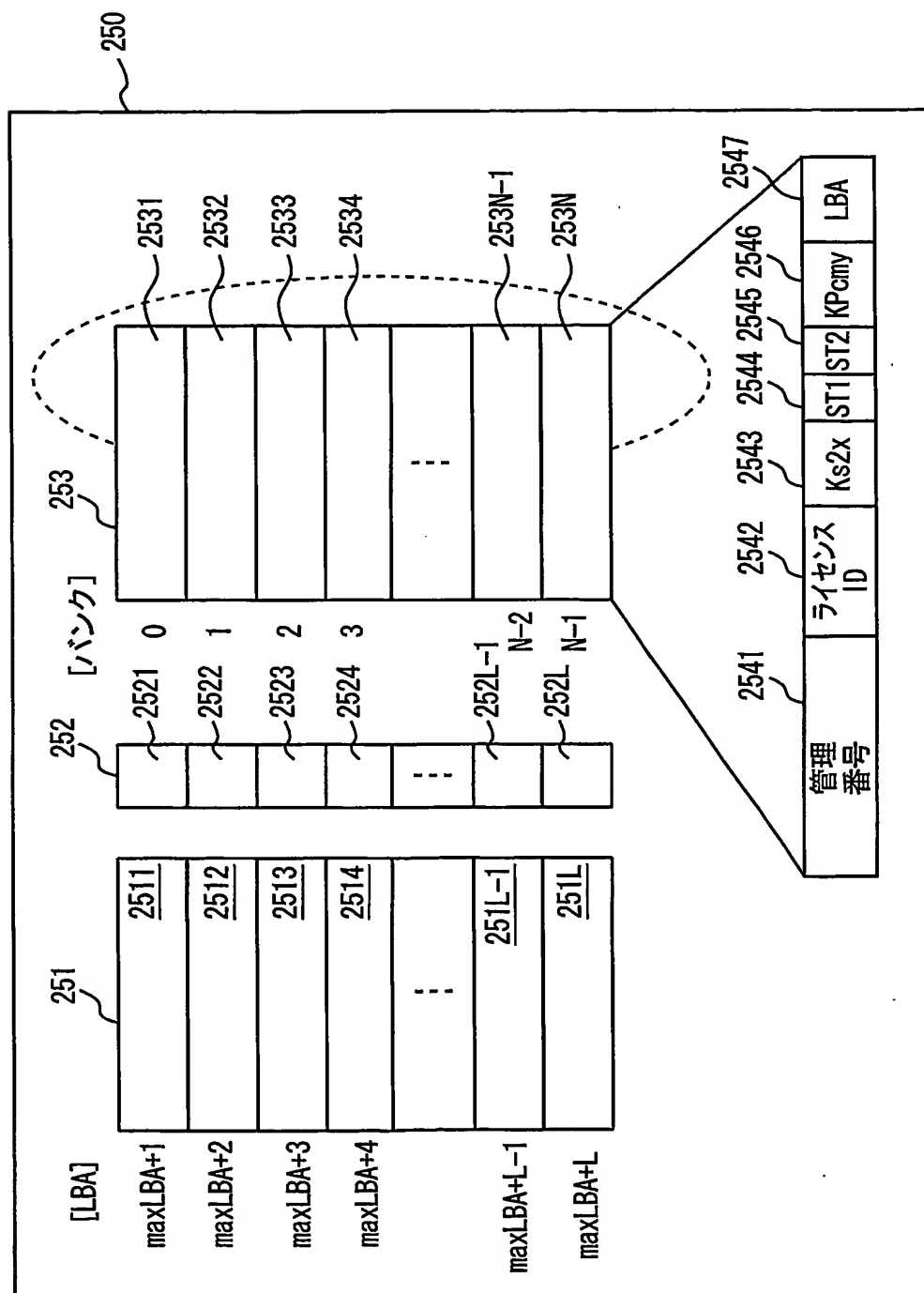


FIG. 8

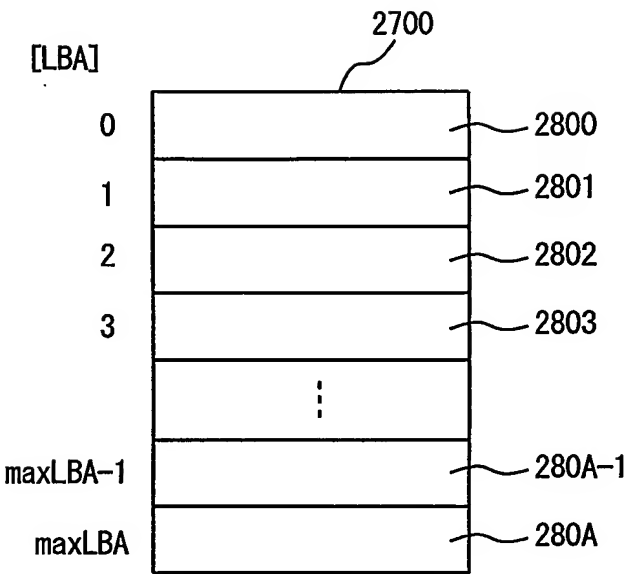


FIG. 9

ライセンス提供装置 40

端末装置 10

HD 20

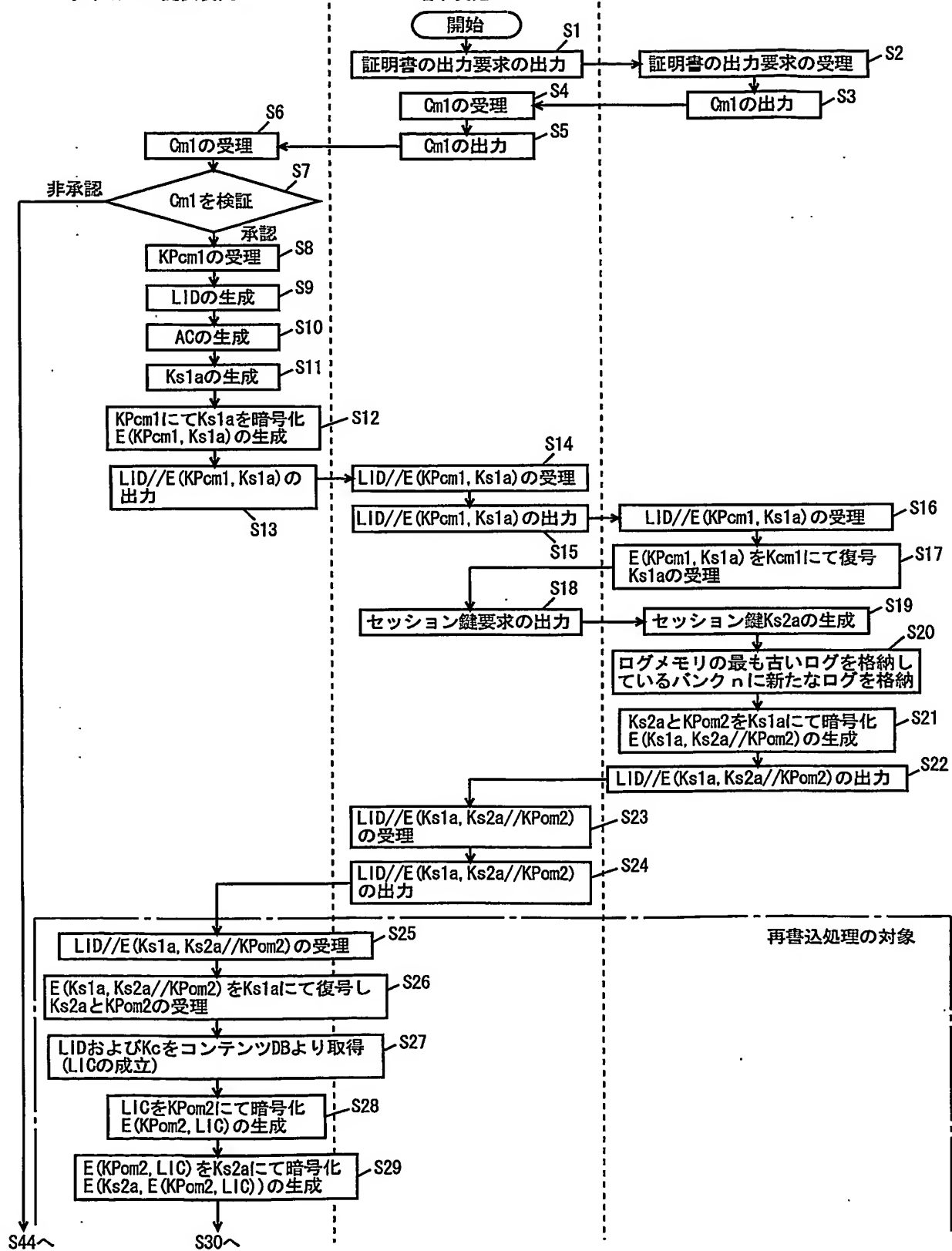


FIG. 10

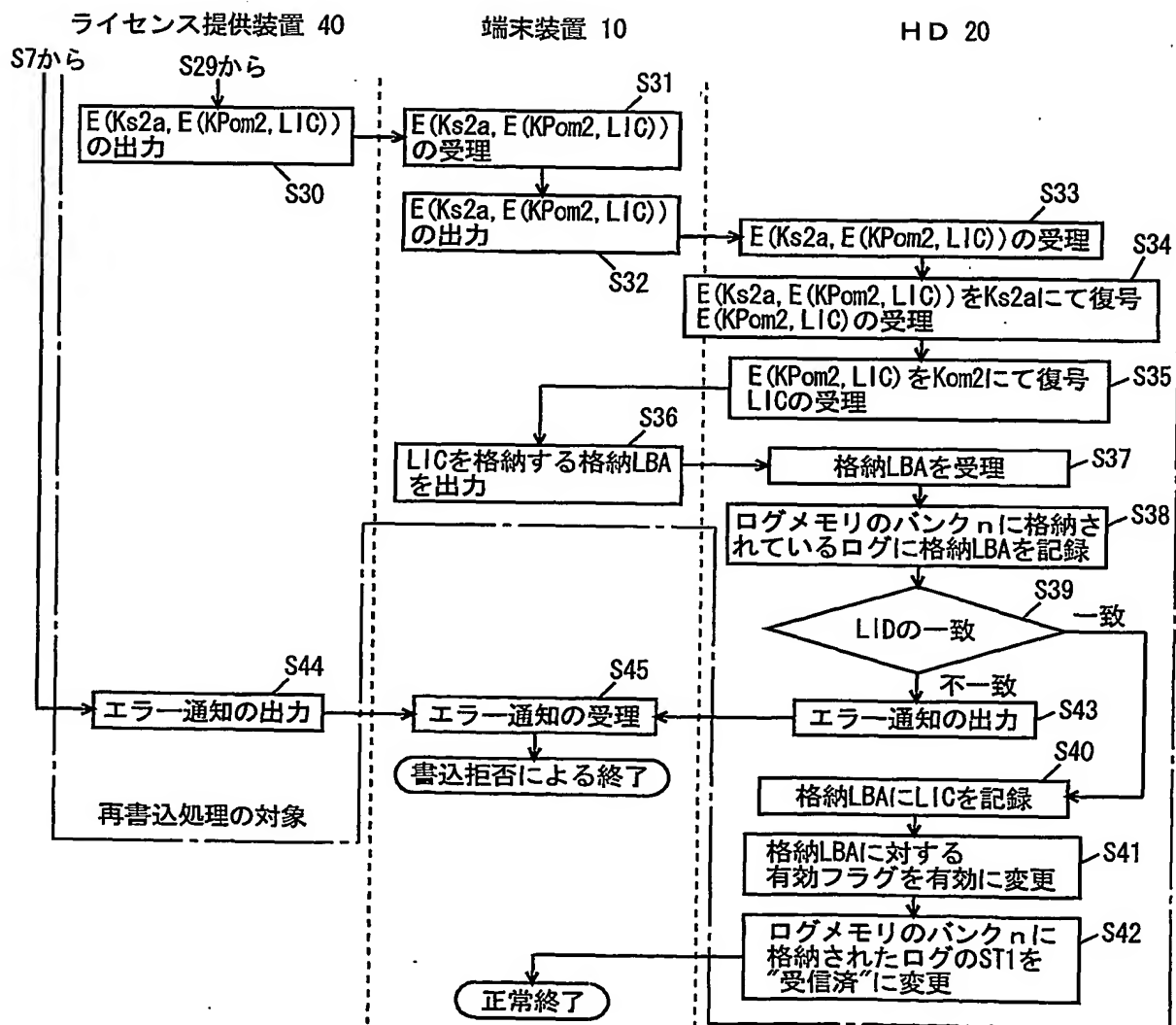


FIG. 11

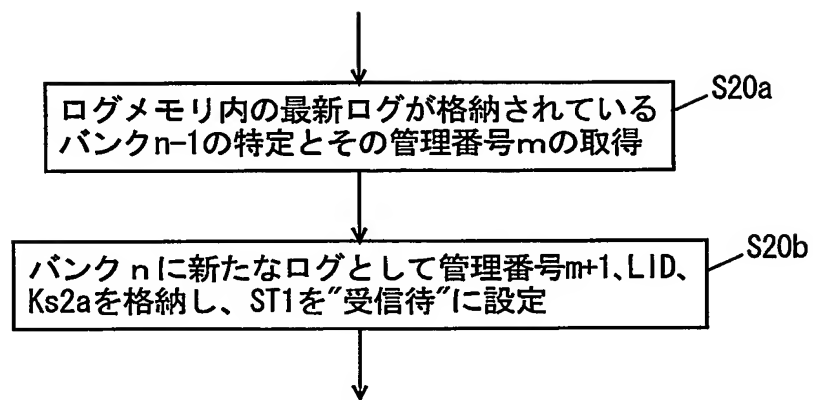


FIG. 12

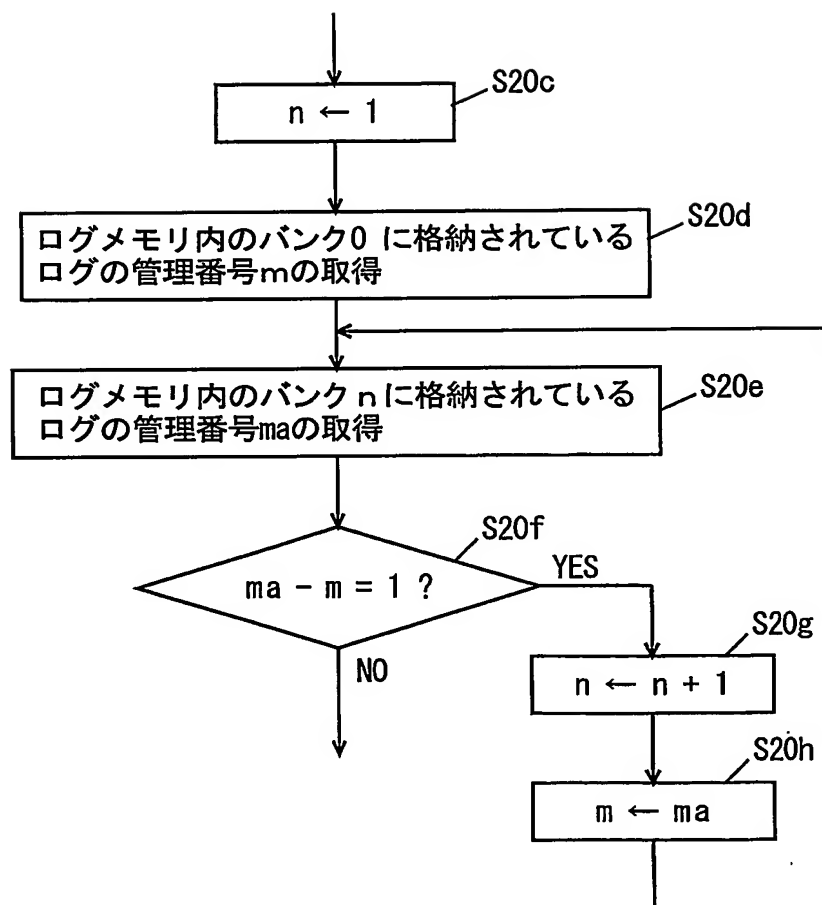


FIG. 13

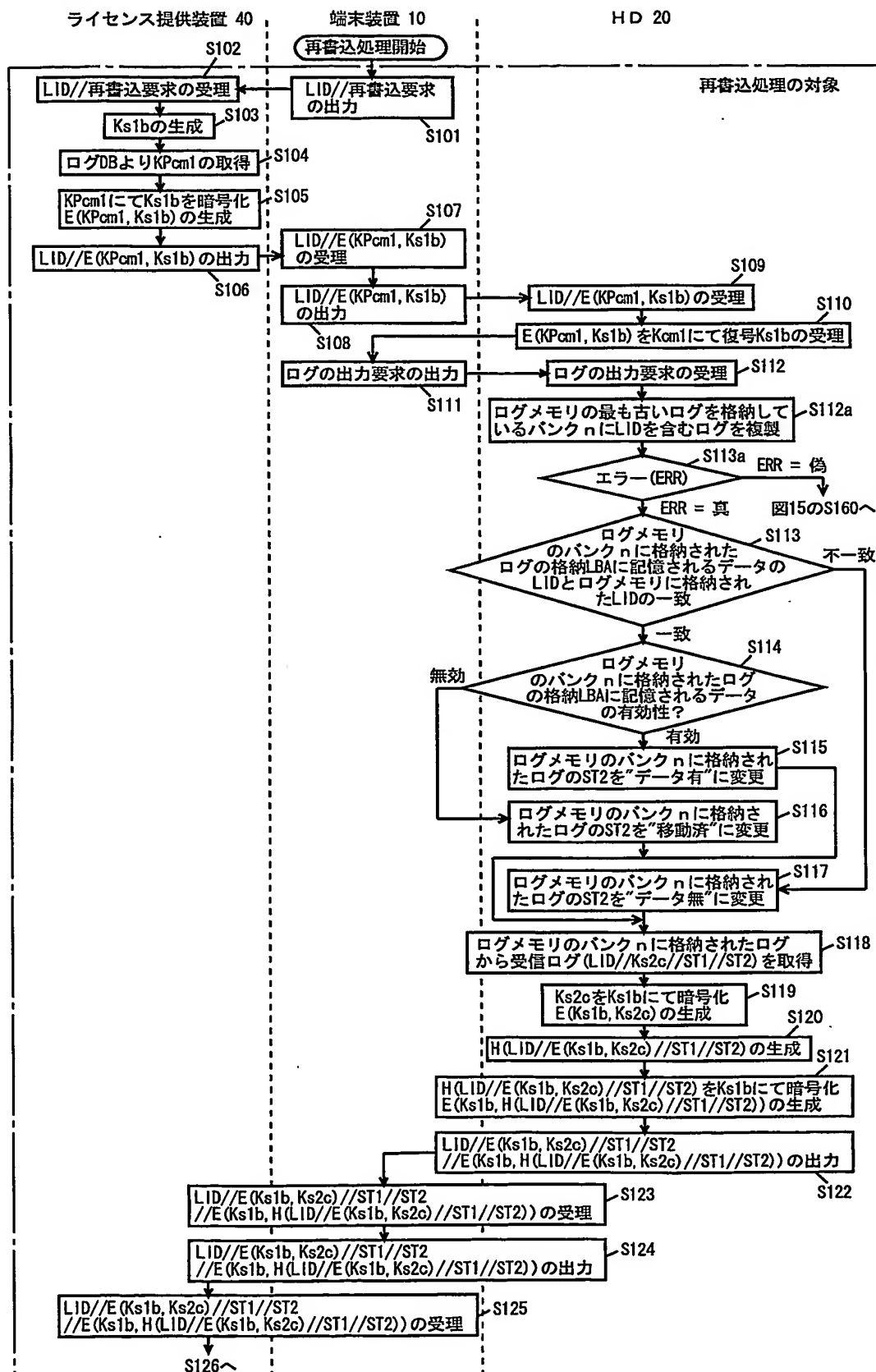


FIG. 14

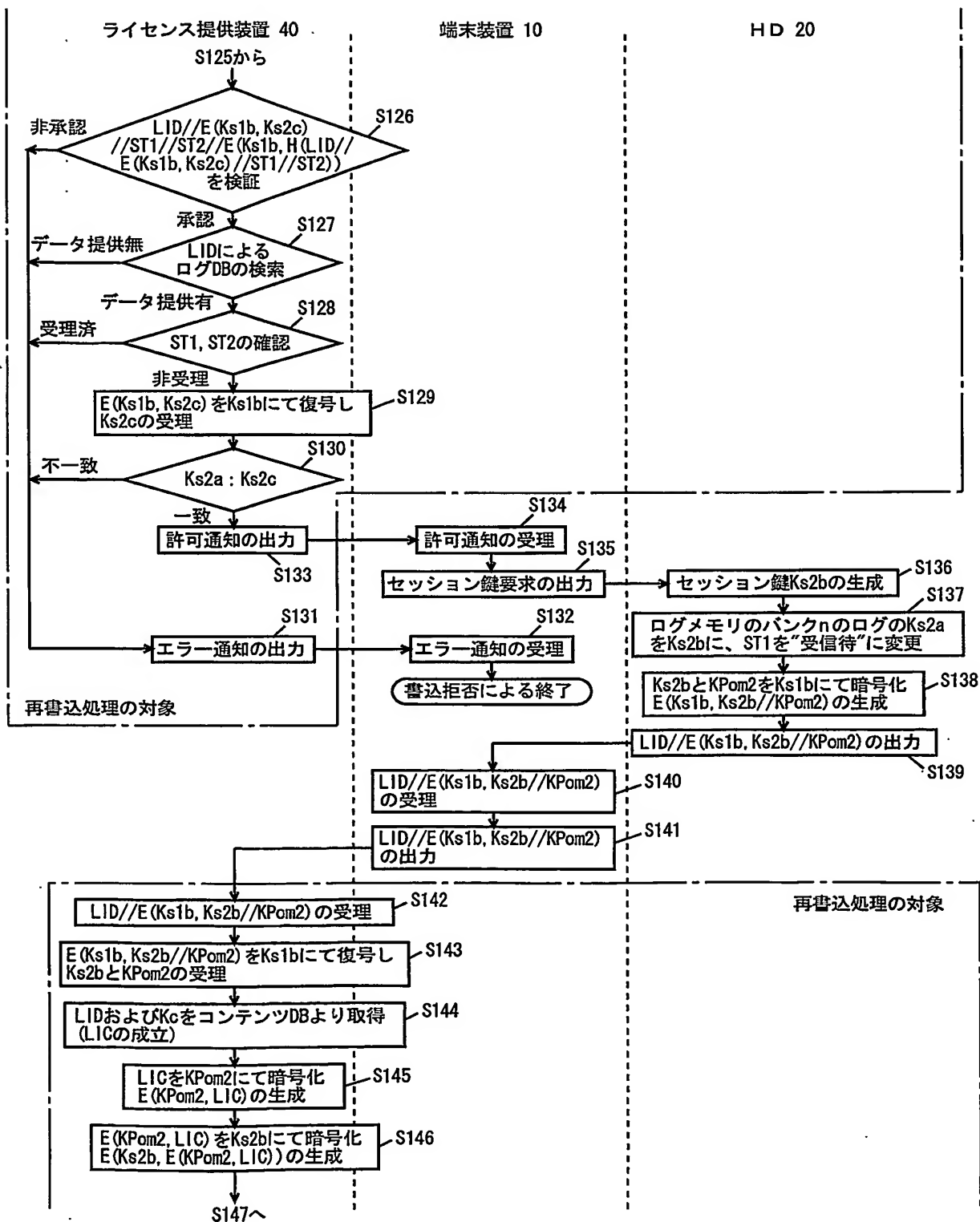


FIG. 15

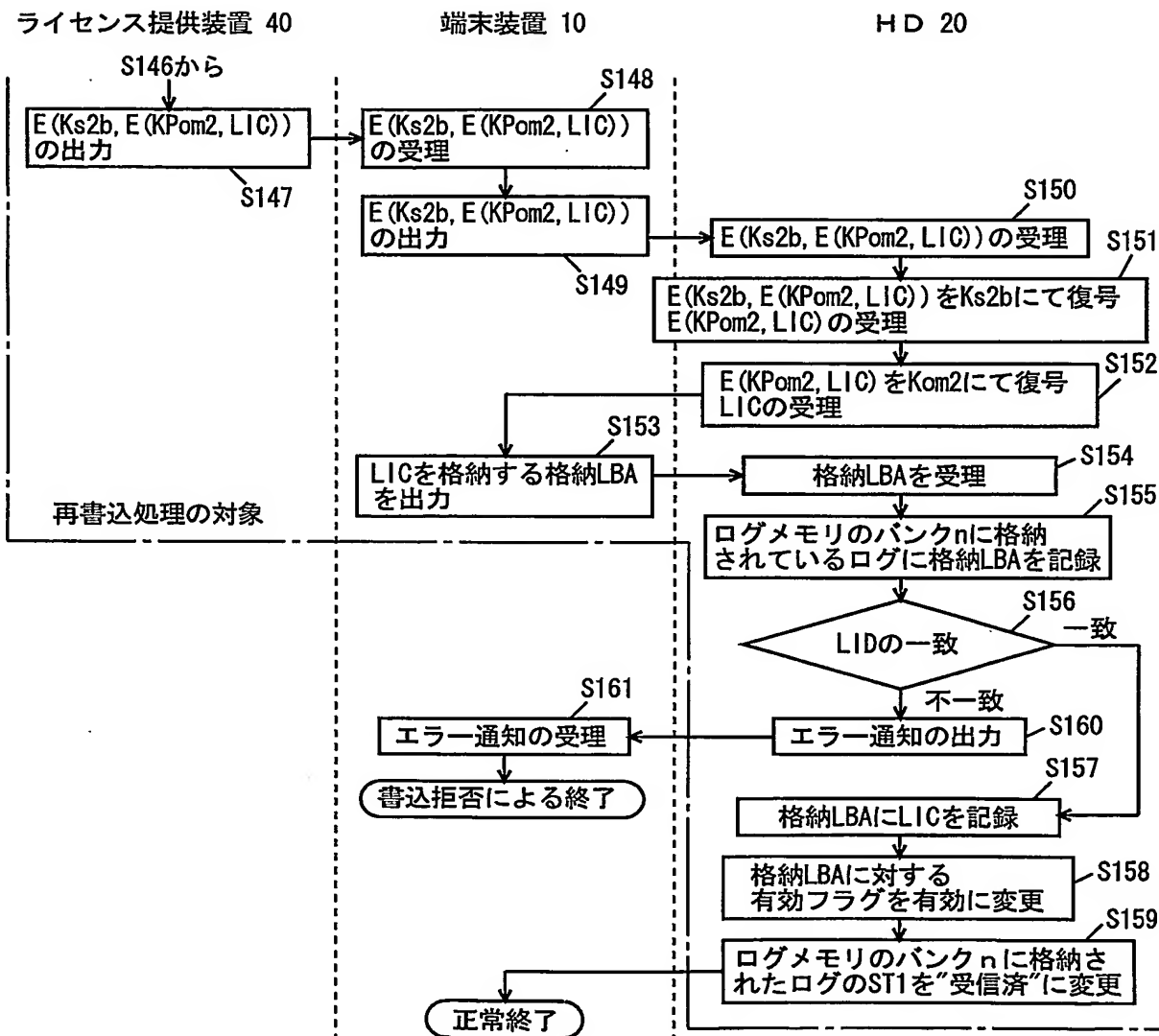


FIG. 16

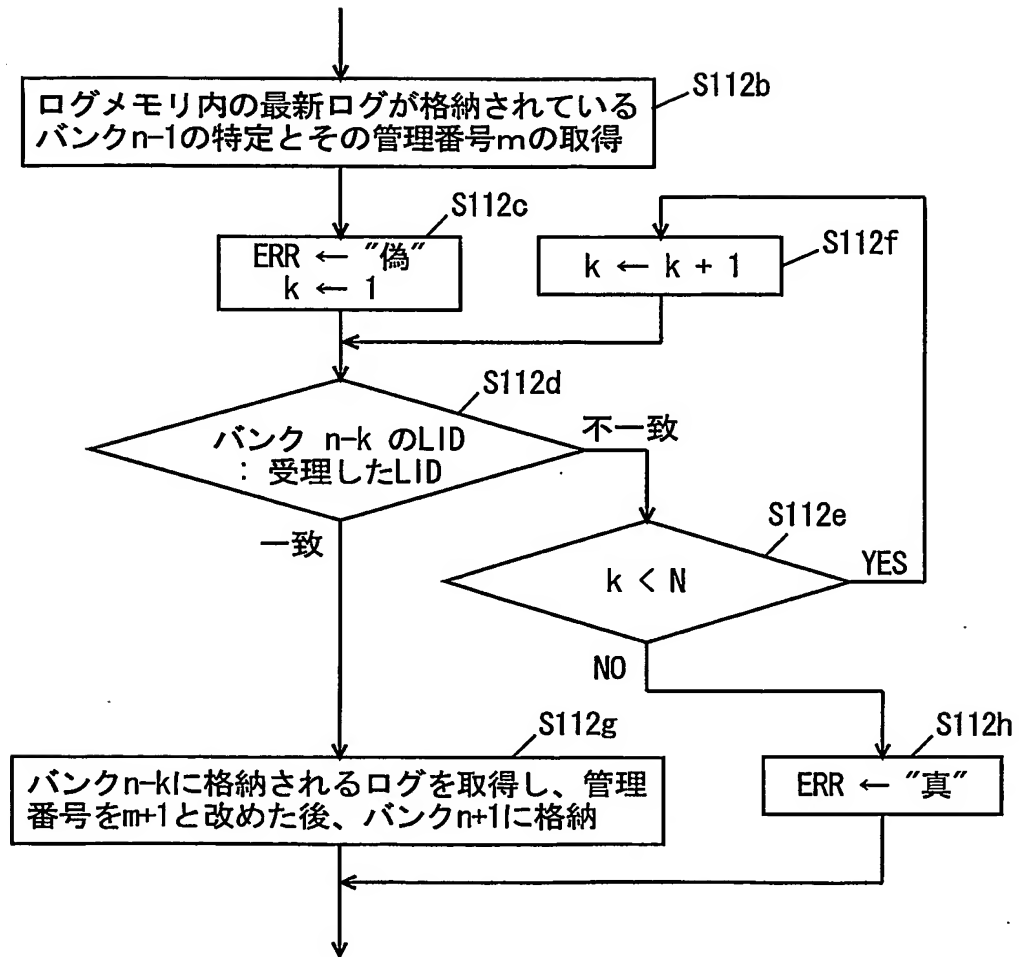


FIG. 17

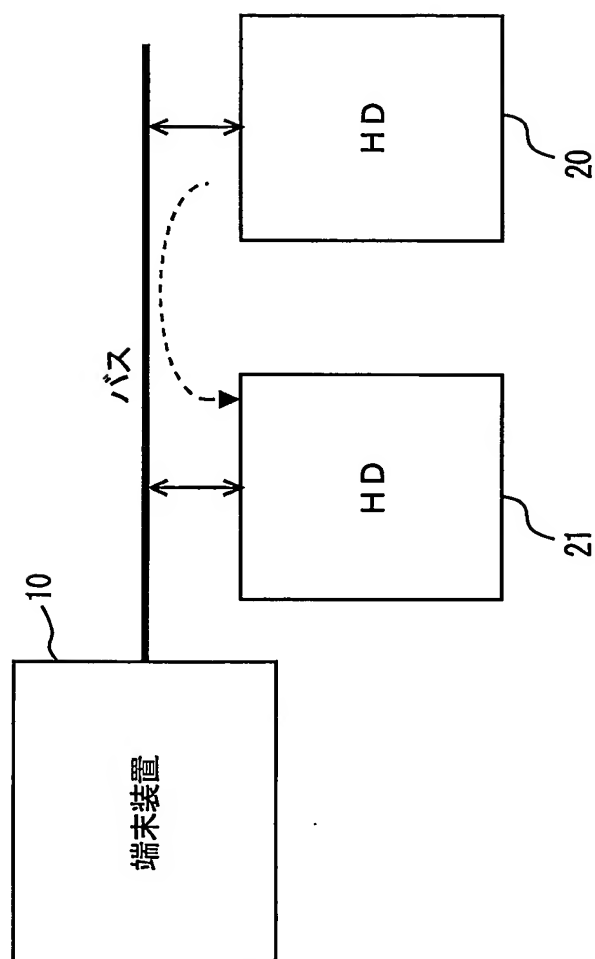


FIG. 18

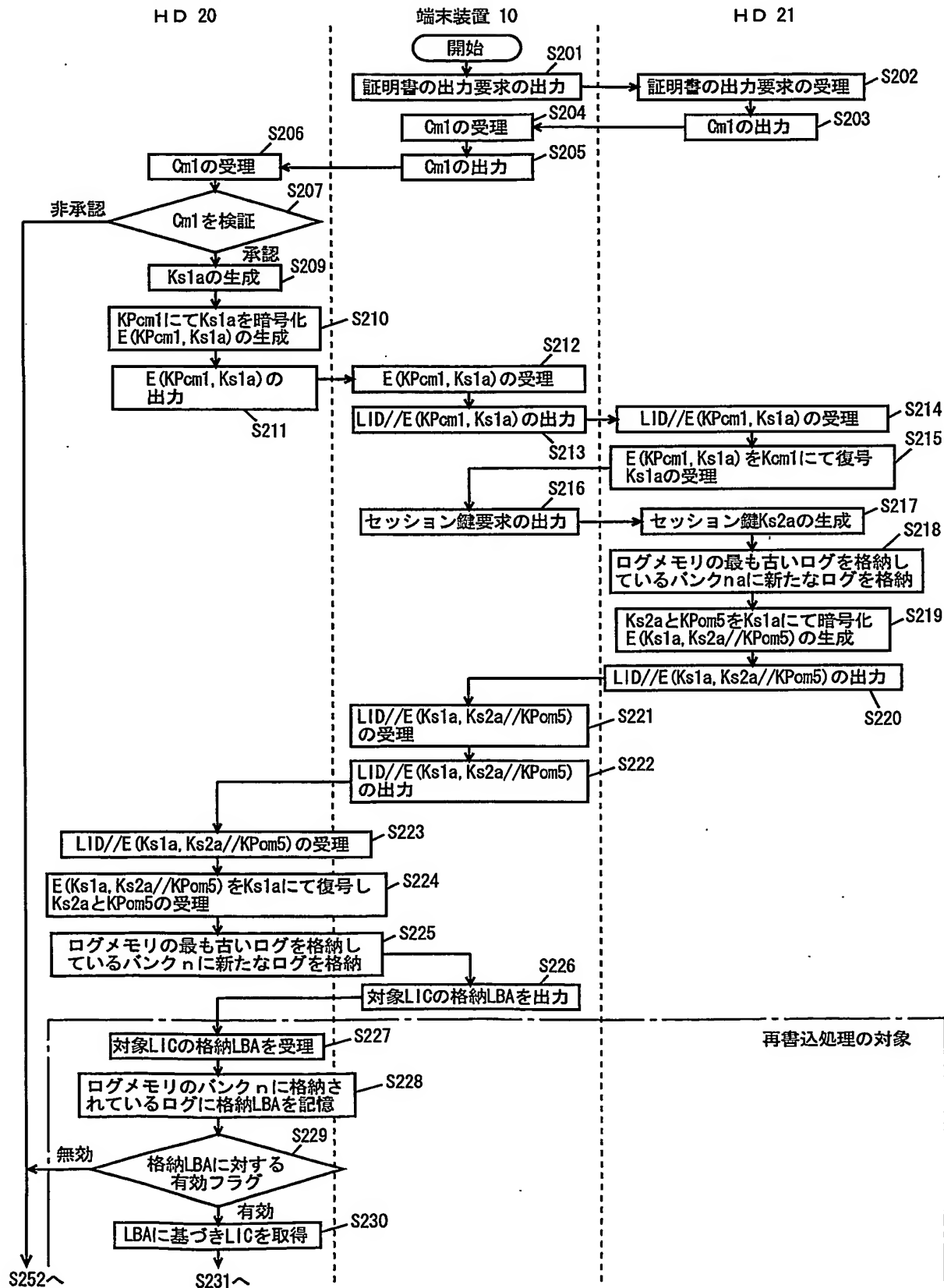


FIG. 19

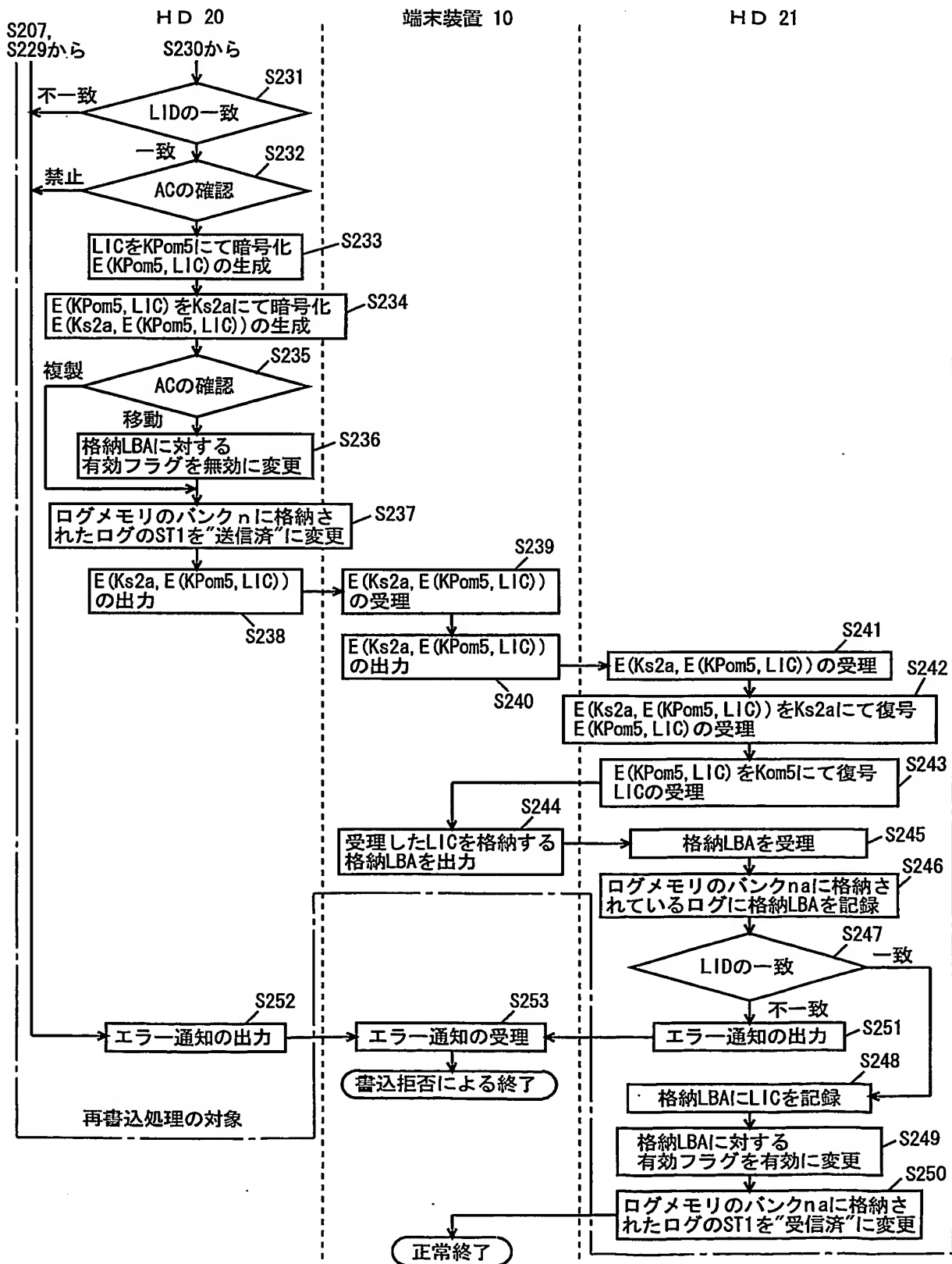


FIG. 20

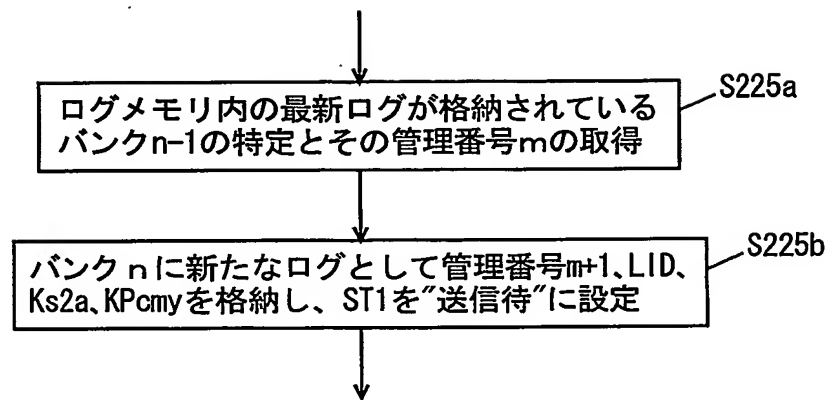


FIG. 21

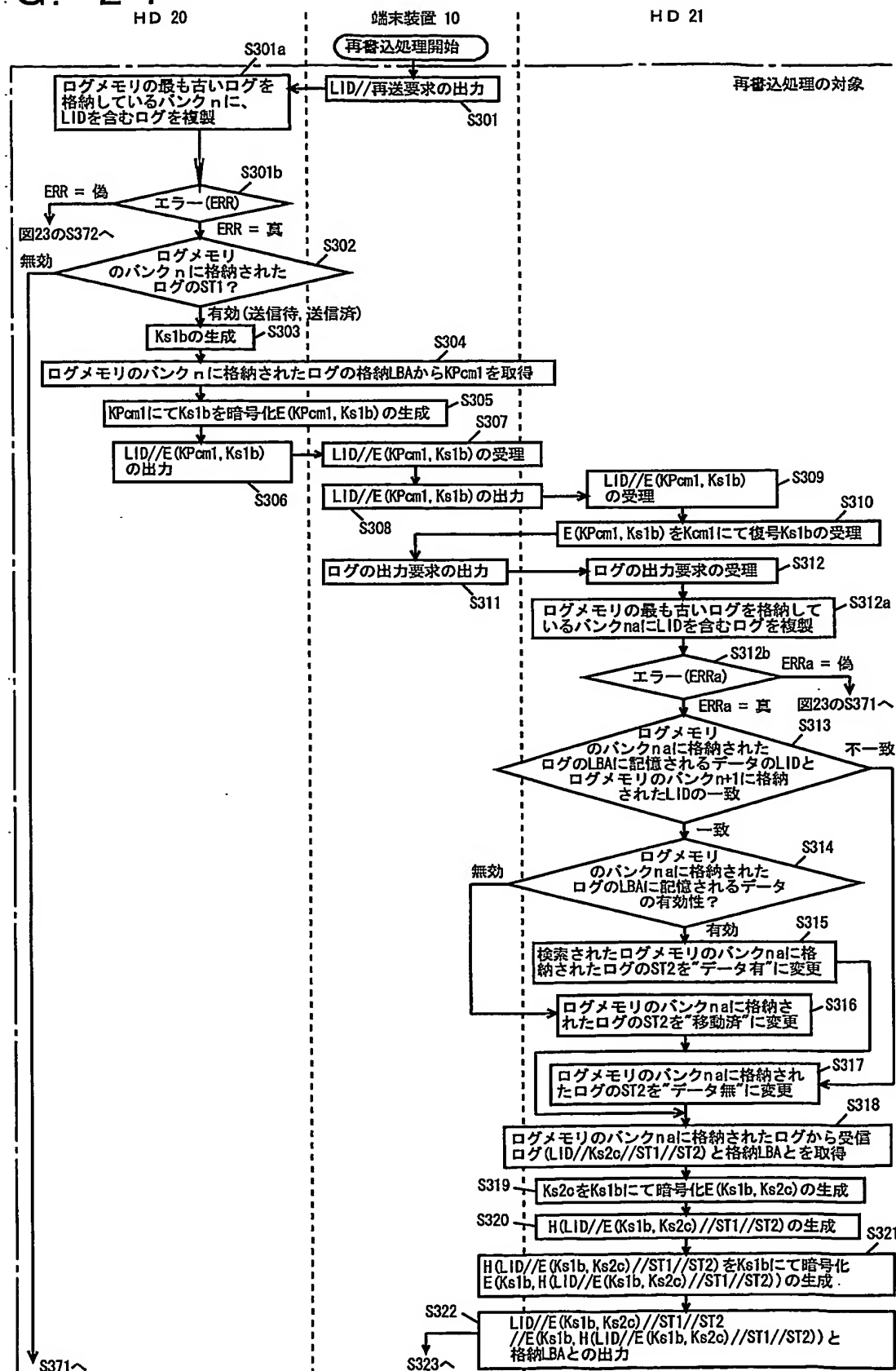
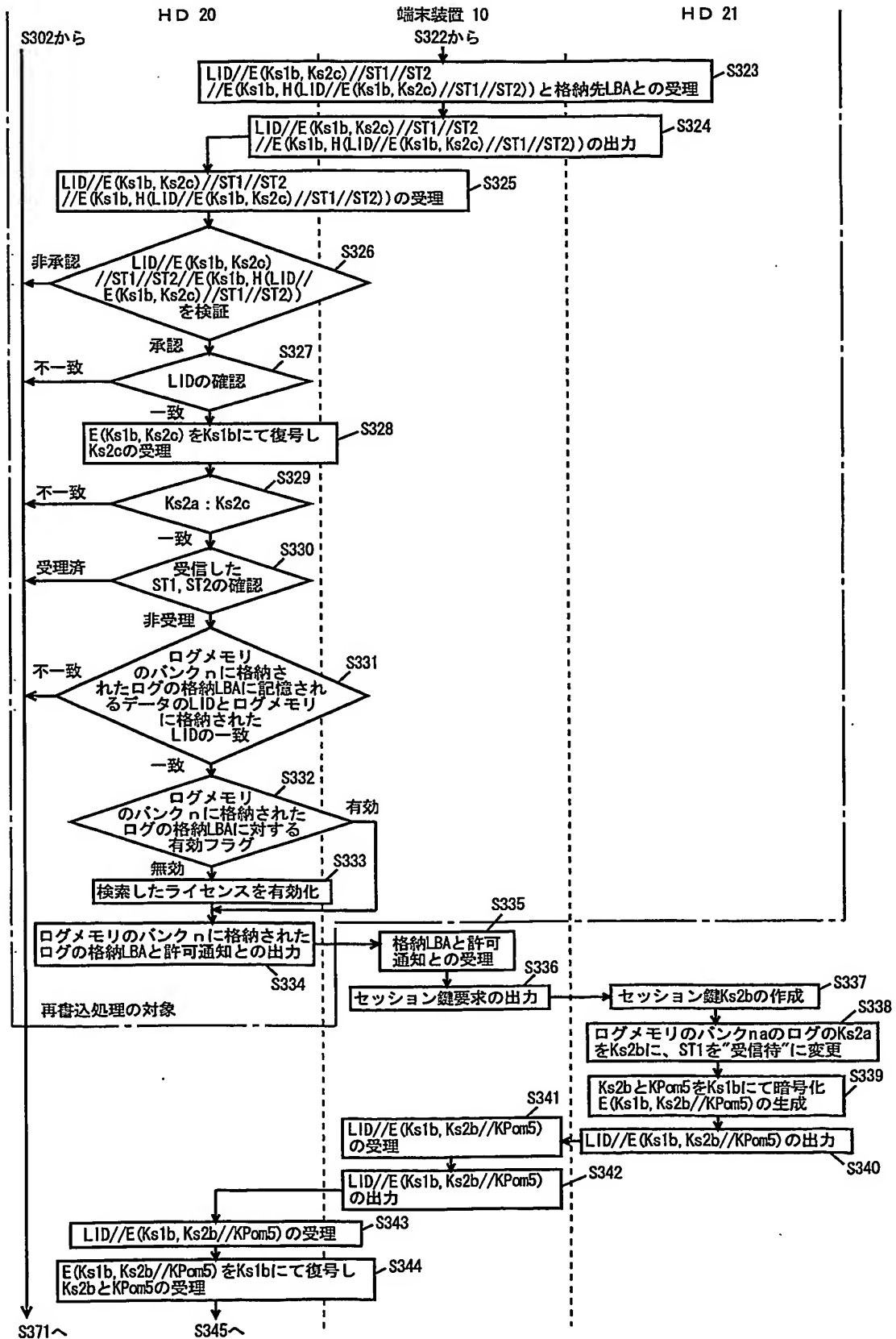


FIG. 22



HD 21



FIG. 24

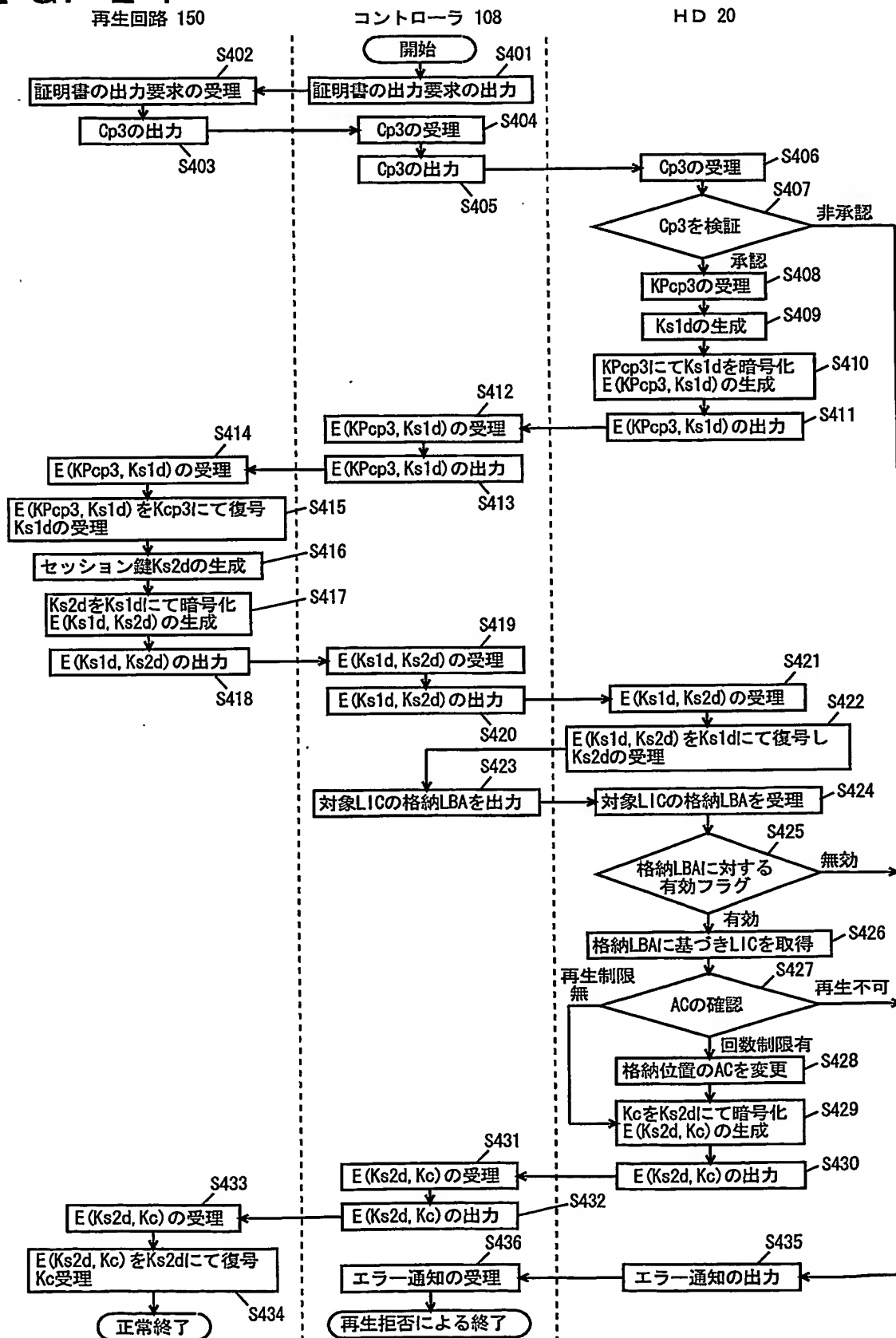


FIG. 25

ライセンス提供装置 40

端末装置 10

HD 20

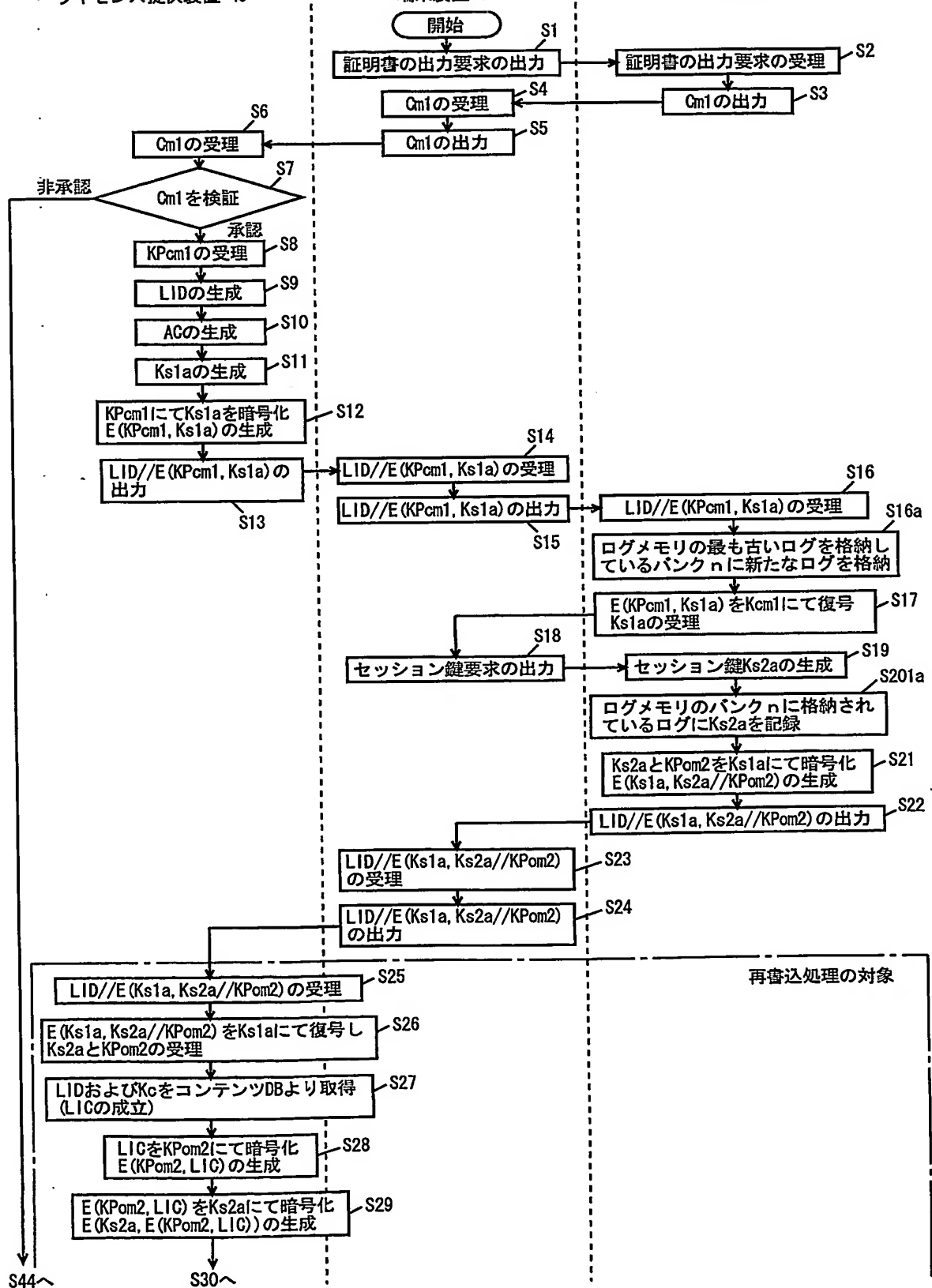


FIG. 26

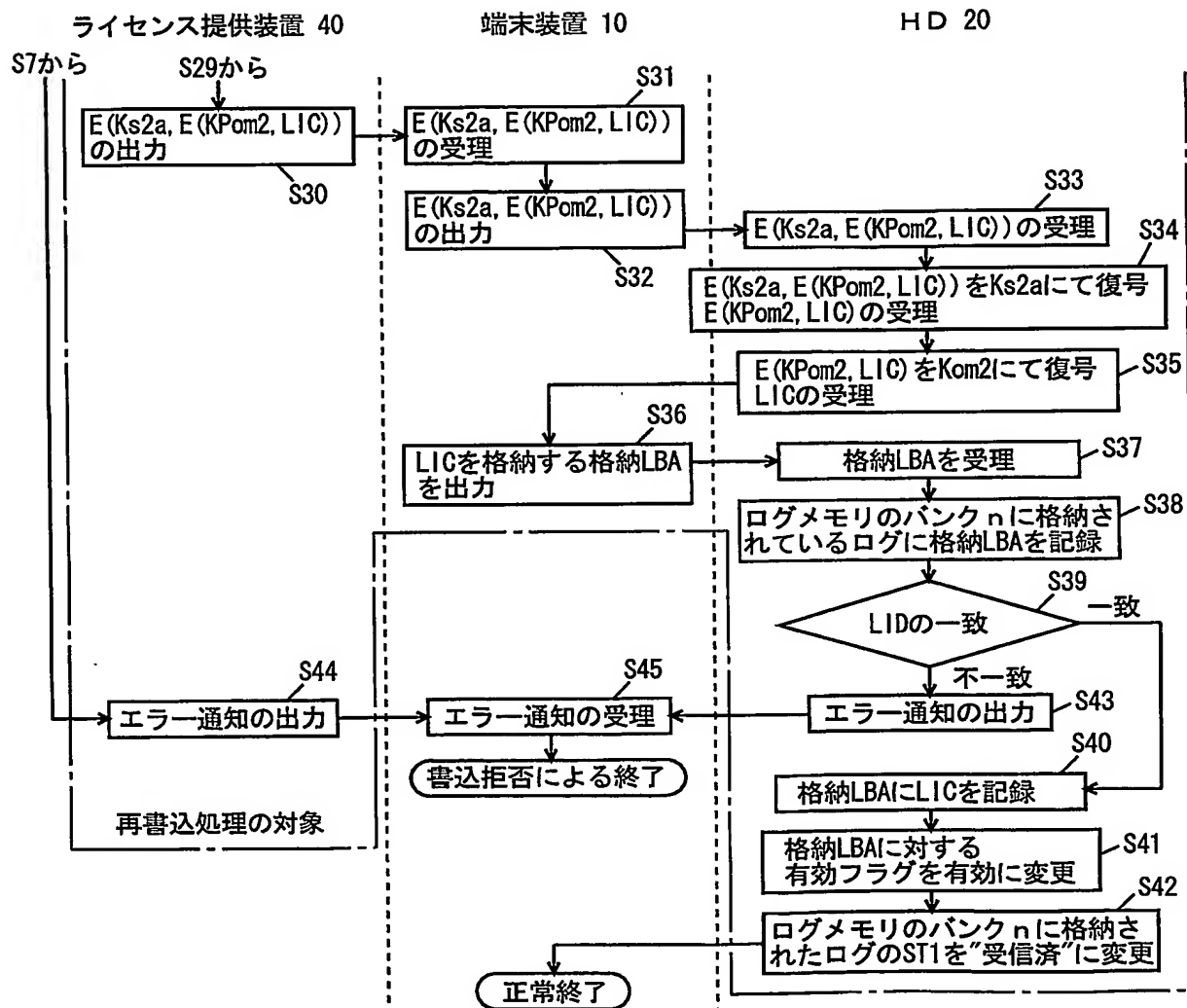


FIG. 27

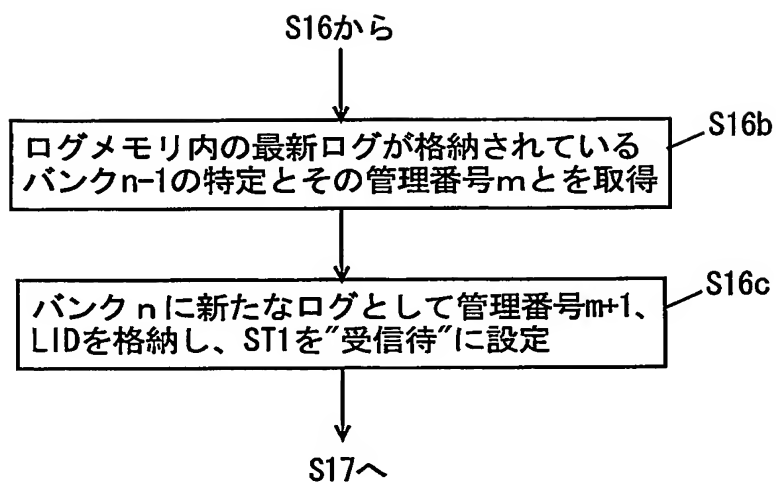


FIG. 28

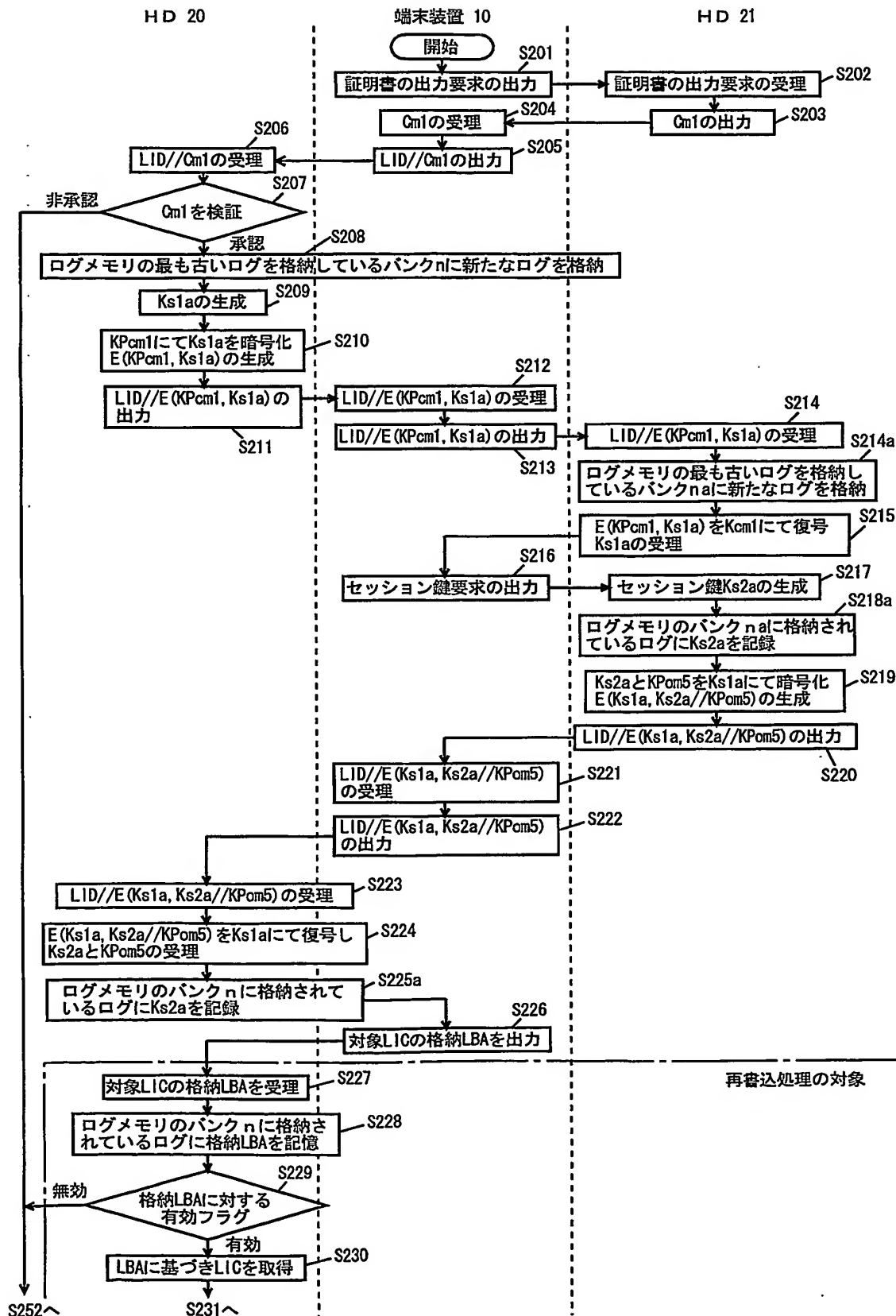


FIG. 29

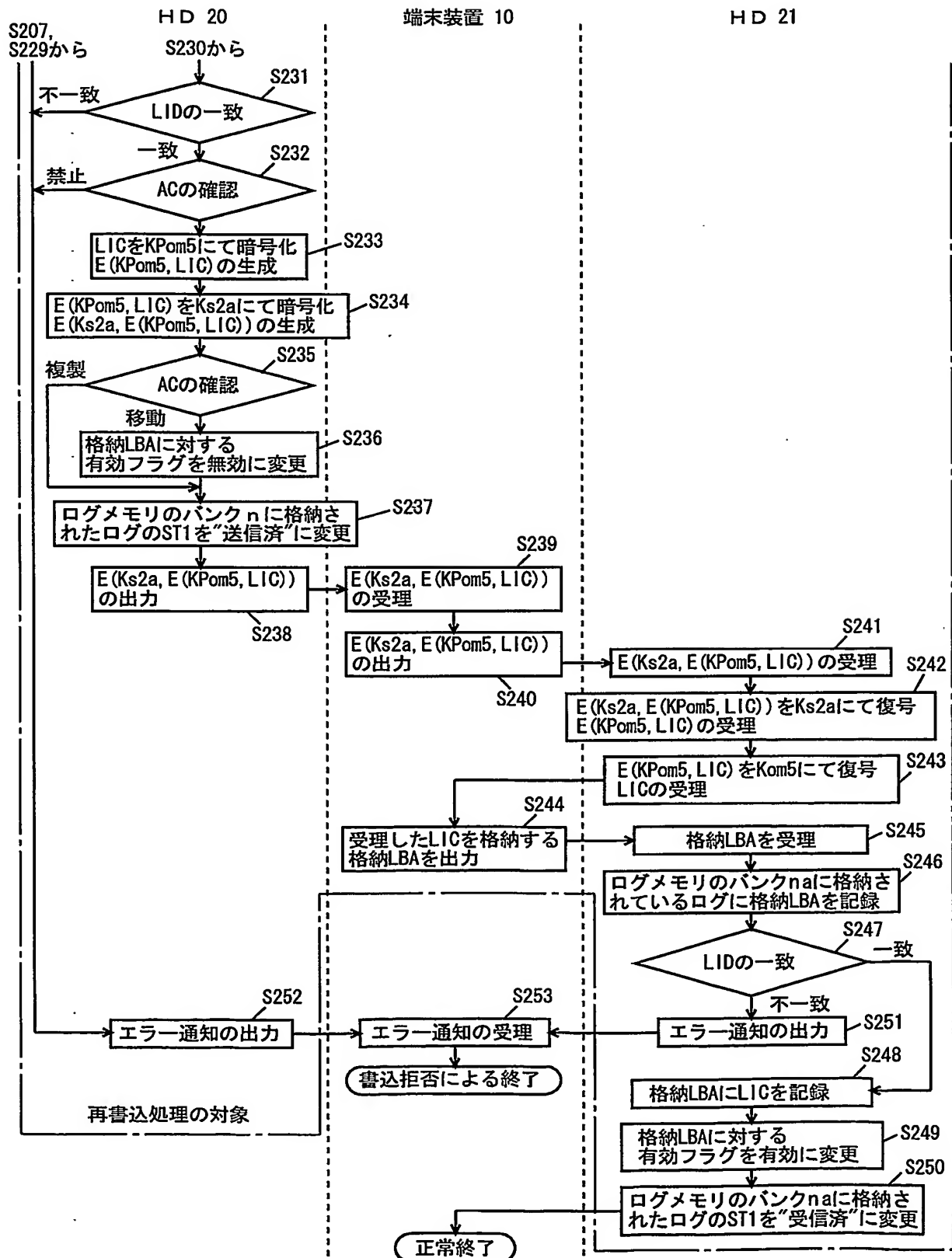
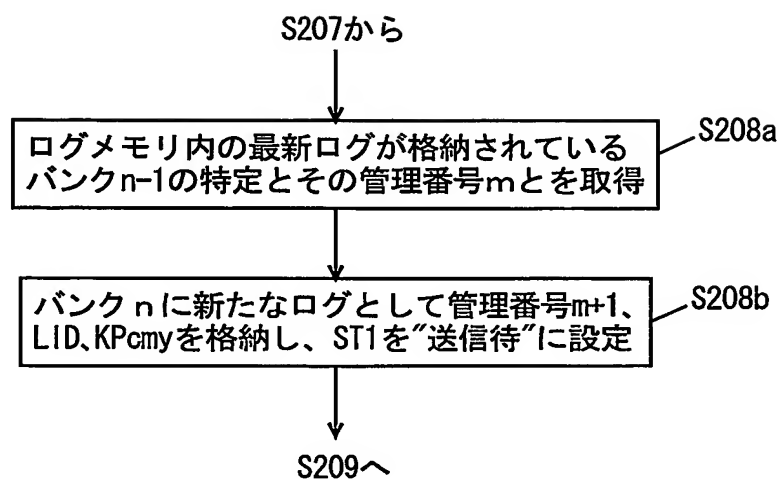


FIG. 30



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/09414

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F12/14, G11B20/10, G06F3/06, H04N5/91

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F12/14, G11B20/10, G06F3/06, H04N5/91

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 01/41356 A1 (Sanyo Electric Co., Ltd.), 07 June, 2001 (07.06.01), All drawings; all pages; in particular, description, page 5 & EP 1237324 A1	1-9
Y	JP 2002-189648 A (Hitachi, Ltd.), 05 July, 2002 (05.07.02), All pages; all drawings; in particular, Par. Nos. [0025] to [0029] (Family: none)	1-9
Y	JP 2001-197292 A (Konica Corp.), 19 July, 2001 (19.07.01), All pages; all drawings; in particular, Par. No. [0052] (Family: none)	1-9

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 15 October, 2003 (15.10.03)	Date of mailing of the international search report 28 October, 2003 (28.10.03)
--	---

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/09414

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 11-39450 A (Mitsubishi Electric Corp.), 12 February, 1999 (12.02.99), All pages; all drawings; in particular, Par. Nos. [0002] to [0005] (Family: none)	1-9
Y	JP 6-202926 A (Fuji Xerox Co., Ltd.), 22 July, 1994 (22.07.94), All pages; all drawings; in particular, Par. No. [0005] (Family: none)	1-9
Y	JP 5-46359 A (Mitsubishi Electric Corp.), 26 February, 1993 (26.02.93), All pages; all drawings; in particular, Fig. 4 (Family: none)	7-9

A. 発明の属する分野の分類 (国際特許分類 (IPC))
Int. Cl.⁷ G06F12/14, G11B20/10, G06F3/06, H04N5/91

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))
Int. Cl.⁷ G06F12/14, G11B20/10, G06F3/06, H04N5/91

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926 - 1996 年
日本国公開実用新案公報 1971 - 2003 年
日本国登録実用新案公報 1994 - 2003 年
日本国実用新案登録公報 1996 - 2003 年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	WO 01/41356 A1 (三洋電機株式会社) 2001.06.07, 全図, 全頁, 特に、明細書第5頁 & EP 1237324 A1	1-9
Y	JP 2002-189648 A (株式会社日立製作所) 2002.07.05, 全頁, 全図, 特に、【0025】 - 【0029】段落 (ファミリーなし)	1-9
Y	JP 2001-197292 A (コニカ株式会社) 2001.07.19, 全頁, 全図, 特に、【0052】段落 (ファミリーなし)	1-9

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

15.10.03

国際調査報告の発送日

28.10.03

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
郵便番号 100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

奥村 元宏

5N

3044

電話番号 03-3581-1101 内線 3585

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 11-39450 A (三菱電機株式会社) 1999. 02. 12, 全頁, 全図, 特に【0002】 - 【0005】 段落 (ファミリーなし)	1-9
Y	JP 6-202926 A (富士ゼロックス株式会社) 1994. 07. 22, 全頁, 全図, 特に【0005】 段落 (ファミリーなし)	1-9
Y	JP 5-46359 A (三菱電機株式会社) 1993. 02. 26, 全頁, 全図, 特に図 4 (ファミリーなし)	7-9